

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Jun EBATA

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: INFORMATION PROVIDING DEVICE, METHOD, PROGRAM AND RECORDING MEDIUM, AND
USER AUTHENTICATION DEVICE, METHOD, PROGRAM AND RECORDING MEDIUM

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

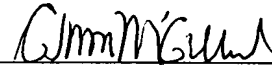
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2003-078993	March 20, 2003
Japan	2004-032085	February 9, 2004

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Marvin J. Spivak

Registration No. 24,913

C. Irvin McClelland

Registration Number 21,124

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 3 月 2 0 日
Date of Application:

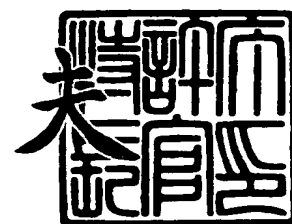
出 願 番 号 特 願 2 0 0 3 - 0 7 8 9 9 3
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 7 8 9 9 3]

出 願 人 株 式 会 社 リ コ ー
Applicant(s):

2 0 0 3 年 1 1 月 2 5 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



出証番号 出証特 2 0 0 3 - 3 0 9 7 1 5 8

【書類名】 特許願

【整理番号】 0301261

【提出日】 平成15年 3月20日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06F 15/00

【発明の名称】 ユーザ認証装置、ユーザ認証方法、ユーザ認証プログラム及び記録媒体

【請求項の数】 21

【発明者】

 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

 【氏名】 江畑 潤

【特許出願人】

 【識別番号】 000006747

 【氏名又は名称】 株式会社リコー

【代理人】

 【識別番号】 100070150

 【弁理士】

 【氏名又は名称】 伊東 忠彦

【手数料の表示】

 【予納台帳番号】 002989

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ユーザ認証装置、ユーザ認証方法、ユーザ認証プログラム及び記録媒体

【特許請求の範囲】

【請求項 1】 ユーザの認証を行う複数の認証手段を連携させる連携手段を有するユーザ認証装置であって、

前記連携手段は、

クライアントからのユーザの第一の認証要求に応じて、第一の認証手段に前記認証要求において指定された第一のユーザ識別情報に基づいて前記ユーザを認証させる第一の呼び出し手段と、

前記クライアントからの、前記第一の認証手段に認証されているユーザの第二の認証要求に応じて、前記第一のユーザ識別情報に予め対応づけられた、第二の認証手段における前記ユーザの第二のユーザ識別情報を検索するユーザ識別情報検索手段と、

前記第二の認証手段に前記ユーザ識別情報検索手段が検索した前記第二のユーザ識別情報に基づいて前記ユーザを認証させる第二の呼び出し手段とを有することを特徴とするユーザ認証装置。

【請求項 2】 前記第一のユーザ識別情報と前記第二のユーザ識別情報とを対応づけて管理するユーザ識別情報対応管理手段を更に有し、

前記ユーザ識別情報検索手段は、前記第一のユーザ識別情報に基づいて前記ユーザ識別情報対応管理手段から前記第二のユーザ識別情報を検索することを特徴とする請求項 1 記載のユーザ認証装置。

【請求項 3】 前記連携手段は、前記第一のユーザ識別情報と前記第二のユーザ識別情報とを対応づけて管理するユーザ識別情報対応管理手段を更に有し、

前記ユーザ識別情報検索手段は、前記第一のユーザ識別情報に基づいて前記ユーザ識別情報対応管理手段から前記第二のユーザ識別情報を検索することを特徴とする請求項 1 記載のユーザ認証装置。

【請求項 4】 前記複数の認証手段の中から前記第一の認証手段を識別する情報を管理する第一の認証手段識別情報管理手段と、

前記複数の認証手段の中から前記第二の認証手段を識別する情報を管理する第二の認証手段識別情報管理手段とを更に有し、

前記第一の呼び出し手段は、前記第一の認証手段識別情報管理手段に基づいて前記第一の認証手段として呼び出す認証手段を識別し、

前記第二の呼び出し手段は、前記第二の認証手段識別情報管理手段に基づいて前記第二の認証手段として呼び出す認証手段を識別することを特徴とする請求項 1 乃至 3 いずれか一項記載のユーザ認証装置。

【請求項 5】 前記認証手段の呼び出し情報が登録された呼び出し情報管理手段を更に有し、

前記第一の呼び出し手段は、前記呼び出し情報管理手段に基づいて前記第一の認証手段を呼び出すことにより、前記第一の認証手段に前記ユーザを認証させ、

前記第二の呼び出し手段は、前記呼び出し情報管理手段に基づいて前記第二の認証手段を呼び出すことにより、前記第二の認証手段に前記ユーザを認証させることを特徴とする 1 乃至 4 いずれか一項記載のユーザ認証装置。

【請求項 6】 前記第一の認証手段は、前記第一の認証手段が前記ユーザを認証したことを証明する電子的な証明書である第一のチケットを生成し、

前記第二の認証手段は、前記第二の認証手段が前記ユーザを認証したことを証明する電子的な証明書である第二のチケットを生成し、

前記ユーザ認証装置は、前記第一の認証要求に対する応答として、前記第一のチケットを前記クライアントに出力し、前記第二の認証要求に対する応答として、前記第二のチケットを前記クライアントに出力することを特徴とする請求項 1 乃至 5 いずれか一項記載のユーザ認証装置。

【請求項 7】 前記連携手段は、前記第一のチケットと前記第二のチケットとをマージするマージチケットを生成するマージチケット生成手段を更に有し、

前記ユーザ認証装置は、前記第一の認証要求に対する応答として、前記第一のチケットがマージされた前記マージチケットを前記クライアントに出力し、前記第二の認証要求に対する応答として、前記第二のチケットがマージされた前記マージチケットを前記クライアントに出力することを特徴とする請求項 6 記載のユーザ認証装置。

【請求項 8】 前記クライアントに出力されたマージチケットは、暗号化されていることを特徴とする請求項 7 記載のユーザ認証装置。

【請求項 9】 前記マージチケット、前記第一のチケット及び前記第二のチケットのうち少なくとも一つは、有効期限を有することを特徴とする請求項 6 乃至 8 いずれか一項記載のユーザ認証装置。

【請求項 10】 前記マージチケット、前記第一のチケット及び前記第二のチケットのうち少なくとも一つは、改竄チェック用のコードを有することを特徴とする請求項 6 乃至 9 いずれか一項記載のユーザ認証装置。

【請求項 11】 前記マージチケット、前記第一のチケット及び前記第二のチケットのうち少なくとも一つは、それぞれが利用可能な対象を示す有効範囲を有することを特徴とする請求項 6 乃至 10 いずれか一項記載のユーザ認証装置。

【請求項 12】 前記第一の認証手段は、パスワードに基づいてユーザの認証を行い、

前記第二の認証手段は、ユーザの指紋に基づいてユーザの認証を行うことを行うことを特徴とする請求項 1 乃至 11 いずれか一項記載のユーザ認証装置。

【請求項 13】 前記連携手段は、

クライアントからの前記マージチケットの解読要求に応じ、前記マージチケットに記録されている情報を前記クライアントが解釈可能な形式にした認証情報データを前記クライアントに出力するチケット解読手段を更に有することを特徴とする請求項 7 乃至 12 いずれか一項記載のユーザ認証装置。

【請求項 14】 前記チケット解読手段は、前記マージチケットにマージされている前記第一のチケットについては前記第一の認証手段に解読させ、前記マージチケットにマージされている前記第二のチケットについては前記第二の認証手段に解読させることを特徴とする請求項 13 記載のユーザ認証装置。

【請求項 15】 前記連携手段の機能は、SOAP の RPC によって呼び出すことが可能なことを特徴とする請求項 1 乃至 14 いずれか一項記載のユーザ認証装置。

【請求項 16】 ユーザの認証を行う複数の認証手段を連携させるユーザ認証装置におけるユーザ認証方法であって

クライアントからのユーザの第一の認証要求に応じて、第一の認証手段に前記認証要求において指定された第一のユーザ識別情報に基づいて前記ユーザを認証させる第一の呼び出し手順と、

前記クライアントからの、前記第一の認証手段に認証されているユーザの第二の認証要求に応じて、前記第一のユーザ識別情報に予め対応づけられた、第二の認証手段における前記ユーザの第二のユーザ識別情報を検索するユーザ識別情報検索手順と、

前記第二の認証手段に前記ユーザ識別情報検索手順において検索された前記第二のユーザ識別情報に基づいて前記ユーザを認証させる第二の呼び出し手順とを有することを特徴とするユーザ認証方法。

【請求項 17】 前記ユーザ識別情報検索手順は、前記第一のユーザ識別情報に基づいて、前記第一のユーザ識別情報と前記第二のユーザ識別情報とを対応づけて管理するユーザ識別情報対応管理手段から前記第二のユーザ識別情報を検索することを特徴とする請求項 16 記載のユーザ認証方法。

【請求項 18】 前記第一の呼び出し手順は、前記複数の認証手段の中から前記第一の認証手段を識別する情報を管理する第一の認証手段識別情報管理手段に基づいて前記第一の認証手段として呼び出す認証手段を識別し、

前記第二の呼び出し手順は、前記複数の認証手段の中から前記第二の認証手段を識別する情報を管理する第二の認証手段識別情報管理手段に基づいて前記第二の認証手段として呼び出す認証手段を識別することを特徴とする請求項 16 又は 17 記載のユーザ認証方法。

【請求項 19】 前記第一の呼び出し手順は、前記認証手段の呼び出し情報が登録された呼び出し情報管理手段に基づいて前記第一の認証手段を呼び出すことにより、前記第一の認証手段に前記ユーザを認証させ、

前記第二の呼び出し手順は、前記呼び出し情報管理手段に基づいて前記第二の認証手段を呼び出すことにより、前記第二の認証手段に前記ユーザを認証させることを特徴とする 16 乃至 18 いずれか一項記載のユーザ認証方法。

【請求項 20】 クライアントからのユーザの第一の認証要求に応じて、第一のユーザ識別情報に基づいて第一の認証手段に前記認証要求において指定され

た前記ユーザを認証させる第一の呼び出し手順と、

前記クライアントからの、前記第一の認証手段に認証されているユーザの第二の認証要求に応じて、前記第一のユーザ識別情報に予め対応づけられた、第二の認証手段における前記ユーザの第二のユーザ識別情報を検索するユーザ識別情報検索手順と、

前記第二の認証手段に前記ユーザ識別情報検索手順において検索された前記第二のユーザ識別情報に基づいて前記ユーザを認証させる第二の呼び出し手順とをコンピュータに実行させるためのユーザ認証プログラム。

【請求項 21】 クライアントからのユーザの第一の認証要求に応じて、第一のユーザ識別情報に基づいて第一の認証手段に前記認証要求において指定された前記ユーザを認証させる第一の呼び出し手順と、

前記クライアントからの、前記第一の認証手段に認証されているユーザの第二の認証要求に応じて、前記第一のユーザ識別情報に予め対応づけられた、第二の認証手段における前記ユーザの第二のユーザ識別情報を検索するユーザ識別情報検索手順と、

前記第二の認証手段に前記ユーザ識別情報検索手順において検索された前記第二のユーザ識別情報に基づいて前記ユーザを認証させる第二の呼び出し手順とをコンピュータに実行させるためのユーザ認証プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ユーザ認証装置、ユーザ認証方法、ユーザ認証プログラム及び記録媒体に関し、特に複数の認証手段を連携させるユーザ認証装置、ユーザ認証方法、ユーザ認証プログラム及び記録媒体に関する。

【0002】

【従来の技術】

情報システムの不正利用を防ぐために、各種アプリケーションは、ユーザの認証機能を有しているのが一般である。認証機能を実現するシステムの具体例とし

てアプリケーションの起動時にユーザIDとパスワードの入力を要求するパスワードシステムが挙げられる。ユーザIDとパスワードとを正しく入力したユーザには、アプリケーションの利用が許可され、以降、ユーザは、アプリケーションが提供する様々な機能を利用することができる。

【0003】

【発明が解決しようとする課題】

しかしながら、ユーザの正当性がアプリケーションの起動時において確認できただけで、そのアプリケーションが提供するすべてのサービスに対する利用権限を与えるのは危険である。例えば、ユーザがアプリケーションを起動したまま席をはずすことがよくある。従って、悪意を持った他のユーザが、正当なユーザに成りすましてアプリケーションを利用することも考えられる。

【0004】

かかる不正利用を防ぐため、例えば企業内の情報システムにおいて管理されている機密情報に対してアクセスする際に、ユーザの認証を再度要求することにより、かかる機密情報に対するセキュリティを高めることができる。

【0005】

この場合、起動時における認証の際に利用した認証エンジン（ユーザ認証を行うためのプログラム）と同一の認証エンジンを利用するよりも、例えば、起動時にはパスワード認証、機密情報へのアクセスの際には指紋認証といったように、全く別の認証エンジンを利用して認証を行ったほうが、より高度なセキュリティを確保することができる。

【0006】

但し、二つ以上の認証エンジンを利用する場合、それぞれがお互いに独立していたのでは意味がない。即ち、一方において認証されたユーザと他方において認証されたユーザとが同一人物であるという保証がないからである。

【0007】

従って、アプリケーションには、複数の認証エンジンを関連づける処理の実装が必要となる。

【0008】

本発明は、上記の点に鑑みてなされたものであって、ユーザの同一性を保証しつつ複数の認証機能によってユーザを認証することができるユーザ認証装置、ユーザ認証方法、ユーザ認証プログラム及び記録媒体の提供を目的とする。

【0009】

【課題を解決するための手段】

そこで上記課題を解決するため、本発明は、ユーザの認証を行う複数の認証手段を連携させる連携手段を有するユーザ認証装置であって、前記連携手段は、クライアントからのユーザの第一の認証要求に応じて、第一の認証手段に前記認証要求において指定された第一のユーザ識別情報に基づいて前記ユーザを認証させる第一の呼び出し手段と、前記クライアントからの、前記第一の認証手段に認証されているユーザの第二の認証要求に応じて、前記第一のユーザ識別情報に予め対応づけられた、第二の認証手段における前記ユーザの第二のユーザ識別情報を検索するユーザ識別情報検索手段と、前記第二の認証手段に前記ユーザ識別情報検索手段が検索した前記第二のユーザ識別情報に基づいて前記ユーザを認証させる第二の呼び出し手段とを有することを特徴とする。

【0010】

このようなユーザ認証装置では、第一の認証手段における第一のユーザ識別情報（ユーザID等）に予め対応づけられた第二のユーザ識別情報に基づいて、第二の認証手段にユーザの認証をさせるため、ユーザの同一性を保証しつつ複数の認証機能によってユーザを認証することができる。

【0011】

また上記課題を解決するため、本発明は、上記ユーザ認証装置におけるユーザ認証方法、又はその方法をコンピュータに行なわせるためのプログラム及び前記プログラムを記録した記録媒体としてもよい。

【0012】

【発明の実施の形態】

以下、図面に基づいて本発明の実施の形態を説明する。図1は、本発明の実施の形態における認証システムの構成例を示す図である。図1に示されるように、本実施の形態における認証システム1は、お互いにインターネットやLAN等の

ネットワークを介して接続されている認証サーバ10と端末10とを有している。

【0013】

端末20はユーザが利用するPC (Personal Computer) 等の端末であり、SOAPプロキシ22、クライアントアプリケーション23、及び指紋読み取り装置ドライバ24等と有している。SOAPプロキシ22は、認証サーバ10との間でSOAP (Simple Object Access Protocol) による通信を実現するためのモジュールであり、クライアントアプリケーション23に対して、認証サーバ10の機能を開数インタフェースとして透過的に提供するためのものである。

【0014】

指紋読み取り装置ドライバ24は、端末20に接続された指紋読み取り装置25に対するインタフェースをクライアントアプリケーション23に提供するためのいわゆるドライバである。指紋読み取り装置25は、ユーザの指紋を読み取るための装置である。

【0015】

クライアントアプリケーション23は、ユーザが直接操作するアプリケーションである。クライアントアプリケーション23は、その起動時やその他のタイミングでユーザの認証が必要になった際に、ユーザに対して認証情報の入力进行を要求する。ユーザによって認証情報が入力されると、クライアントアプリケーション23は、SOAPプロキシ22を介して認証サーバ10にユーザの認証を要求する。

【0016】

クライアントアプリケーション23の種類については、特に限定されないが、少なくとも利用する際に認証を必要とするものである。本実施の形態においては、一般的なものと同様にメール機能等を有するグループウェアのクライアントアプリケーションを想定する。

【0017】

なお、端末20の位置づけ (認証サーバ10のクライアント) としてWebサーバを想定してもよい。この場合、当該Webサーバは、Webアプリケーション

ンとして実装されているクライアントアプリケーション 23 と、SOAP プロキシ 22 を有し、SOAP プロキシ 22 によって認証サーバ 10 との通信を行う。当該 Web サーバの Web クライアントとしてユーザが利用する端末には、Web ブラウザと、指紋読み取り装置ドライバ 24 が実装され、更に、指紋読み取り装置 25 が接続されていればよい。こうすることによって、ユーザは、クライアントアプリケーション 23 の機能を、端末の Web ブラウザに表示された Web ページを通して利用することができる。

【0018】

ユーザがクライアントアプリケーション 23 を起動すると、クライアントアプリケーション 23 は、まずユーザ ID（ユーザ識別情報）とパスワードの入力を要求する。ユーザがユーザ ID とパスワードとを入力すると、クライアントアプリケーション 23 は、SOAP プロキシ 22 を介して認証サーバ 10 に対しユーザの認証を要求する。また、ユーザがクライアントアプリケーション 23 上において、指紋認証が必要とされるセキュリティレベルの高い操作を行うとすると、クライアントアプリケーション 23 は、ユーザに対して指紋の入力を要求する。ユーザが指紋読み取りデバイス 25 によって指紋を入力すると、クライアントアプリケーション 23 は、認証サーバ 10 に対し、ユーザの認証を要求する。

【0019】

一方、認証サーバ 10 は、ユーザ認証のサービスを Web サービスとして提供するコンピュータであり、認証サービスモジュール 11 がインストールされている。

【0020】

認証サービスモジュール 11 は、認証サーバ 10 をユーザ認証サービスの提供をするための装置として機能させるためのソフトウェアであり、本実施の形態においては、SOAP スタブ 12、プロバイダ呼び分け手段 13、認証プロバイダ A 14、認証プロバイダ B 15、パスワード・指紋マージプロバイダ 16、パスワード認証プロバイダ 17、指紋認証プロバイダ 18、及びマージ情報管理 DB 19 等から構成されている。

【0021】

SOAPスタブ12は、端末20との間でSOAPによる通信を実現するためのモジュールである。プロバイダ呼び分け手段13は、端末20に対して、後述する各種認証プロバイダに対する共通のインタフェースを提供するためのモジュールである。プロバイダ分け手段13は、端末20からユーザの認証要求を受けると、当該認証要求において指定された認証プロバイダを呼び出す。

【0022】

認証プロバイダA14、認証プロバイダB15、パスワード・指紋マージプロバイダ16、パスワード認証プロバイダ17、及び指紋認証プロバイダ18等は、「認証プロバイダ」と呼ばれるモジュールである。ここで、認証プロバイダとは、様々な認証エンジンを認証サービスモジュール11に組み込むためのアダプタ、又は仲介者のような役割を果たすものである。なお、認証エンジンとは、ここでは実際にパスワードの照合や、指紋の照合等の認証処理を行うシステムをいう。

【0023】

即ち、個々の認証エンジンは、それぞれ独自のインタフェース（プロトコル）を有している。一方、それぞれの認証エンジンにおける認証機能をWebサービスとして端末20等に提供するにはプロバイダ呼び分け手段13との間で規定される所定のインタフェースに従う必要がある。かかる個々の認証エンジンによる独自のプロトコルを吸収し、プロバイダ呼び分け手段13に対して共通のインタフェースを提供するのが、認証プロバイダである。従って、新たな認証エンジンを認証サービスモジュール11に組み込むには、認証プロバイダを一つ実装することになる。但し、認証プロバイダ自身が、認証エンジンとしての機能を有しているもよい。

【0024】

具体的には、パスワード認証プロバイダ17は、パスワード認証を行うための認証エンジンが実装されているサーバである外部認証サーバ40の認証機能をWebサービスとして提供するための認証プロバイダである。また、指紋認証プロバイダ18は、指紋認証ライブラリ181と指紋DB182とによる指紋認証機能をWebサービスとして提供するための認証プロバイダである。指紋認証ライ

ブラリ 181 は、指紋認証に関する機能を提供する関数群である。また、指紋 DB 182 は、ユーザ毎の指紋特徴データが登録されているデータベースである。

【0025】

認証プロバイダ A 14 及び認証プロバイダ 15 は、様々な認証プロバイダを実装することが可能であることを示すための例示である。

【0026】

パスワード・指紋マージプロバイダ 16 は、認証プロバイダの一つであるが、認証エンジンに対する直接の仲介役として機能するものではないという点において、他の認証プロバイダとは異なる。即ち、パスワード・指紋マージプロバイダ 16 は、パスワード認証プロバイダ 17 と指紋認証プロバイダ 18 とを連携させるための機能を提供する認証プロバイダである。なお、パスワード・指紋マージプロバイダ 16 のように複数の認証プロバイダを連携させるための認証プロバイダを、以下「マージプロバイダ」と呼ぶ。

【0027】

マージプロバイダによって連携される認証プロバイダは、それぞれ対等な関係ではなく主従関係を持つ。ここで、「主」となる認証プロバイダを「プライマリ(primary)プロバイダ」と呼び、「従」となる認証プロバイダを「追加(additional)プロバイダ」と呼ぶこととする。連携された認証プロバイダの中で、プライマリプロバイダは一つであり、それ以外は全て追加プロバイダとなる。

【0028】

ここで、主従の関係と表現したのは、追加プロバイダによって認証する際には、プライマリプロバイダによって既に認証されていることが前提となるからである。逆に、プライマリプロバイダによって認証する際は、追加プロバイダによって認証されていることは前提とならない。即ち、最初の認証に利用されるのがプライマリプロバイダであり、プライマリプロバイダによって認証が済んでいる場合において、更に特別な認証が必要な際に利用されるのが追加プロバイダというわけである。即ち、「連携」とは、複数の認証プロバイダを、上記の主従関係を持たせて結合することをいう。

【0029】

本実施の形態においては、パスワード認証プロバイダ17をプライマリプロバイダとし、指紋認証プロバイダ18を追加プロバイダとした例について説明する。なお、マージプロバイダも、他の認証プロバイダと同様に、複数存在させてもよく、マージプロバイダによってマージする認証プロバイダの組み合わせは自由である。例えば、認証プロバイダA14と認証プロバイダ15とをマージする新たなマージプロバイダを定義してもよいし、パスワード・指紋マージプロバイダ16に認証プロバイダA14を更にマージさせてもよい。

【0030】

マージ情報管理DB19は、認証サーバ10に実装されている認証プロバイダの一覧や、認証プロバイダ同士のマージの関係が登録されているデータベースである。

【0031】

ここで、マージ情報管理DB19を構成する各種テーブルについて説明する。図2は、マージ情報管理DBを構成する認証プロバイダ管理テーブルの構成例を示す図である。図2の認証プロバイダ管理テーブル191（呼び出し情報管理手段）は、認証サーバ10に登録されている認証プロバイダの一覧を管理しているテーブルであり、認証プロバイダ毎に、プロバイダ名、実装名、及び実装依存の初期化情報等が登録されている。

【0032】

プロバイダ名は、認証プロバイダを一意に識別するための名前である。実装名は、例えば認証プロバイダの実装されているファイル名（EXE名、DLL名）、及び関数名等、認証プロバイダを呼び出すために、あるいは起動するために必要となる情報である。実装依存の初期化情報は、認証プロバイダの呼び出し時、又は起動時に必要となる情報である。

【0033】

このように、認証プロバイダ管理テーブル191によって、各認証プロバイダの呼び出し情報を管理することにより、プロバイダ呼び分け手段13と認証プロバイダ、及びマージプロバイダと当該マージプロバイダにマージされる認証プロ

バイダとの間の結合を動的なものとすることができる。即ち、プロバイダ呼び分手段 13 やマージプロバイダのソースコードには、呼び出し情報に依存する定義（例えば、ロードする DLL 名や、呼び出す関数名等）をハードコーディングしておく必要はない。従って、新たな認証プロバイダを追加した場合でも、当該認証プロバイダが所定のインタフェースに従っている限り、プロバイダ呼び分け手段 13 やマージプロバイダのソースコードを修正する必要はない。

【0034】

本実施の形態においては、上述したように、認証プロバイダ A 14、認証プロバイダ B 15、パスワード・指紋マージプロバイダ 16、パスワード認証プロバイダ 17、及び指紋認証プロバイダ 18 等が存在するため、それぞれのレコードが認証プロバイダ管理テーブル 191 に登録されている。

認証プロバイダ管理テーブル 191 によって、例えばプロバイダ呼び分け手段 13 は、端末 20 からユーザの認証要求があった際に、対応する認証プロバイダを呼び出すための手続きを知ることができる。

【0035】

また、図 3 は、マージ情報管理 DB を構成するマージプロバイダ管理テーブルの構成例を示す図である。図 3 のマージプロバイダ管理テーブル 192（第一の認証手段識別情報管理手段）は、認証プロバイダ管理テーブル 191 に登録されている認証プロバイダのうち、マージプロバイダである認証プロバイダを管理するテーブルであり、マージプロバイダ毎に、マージプロバイダ名及びプライマリプロバイダ名等が登録されている。

【0036】

マージプロバイダ名は、マージプロバイダのプロバイダ名である。プライマリプロバイダ名は、当該マージプロバイダにおいてプライマリプロバイダとなっているプロバイダ名である。

【0037】

マージプロバイダ管理テーブル 192 によって、マージプロバイダを識別することができる。また、マージプロバイダは、マージプロバイダ管理テーブル 192 によって、自身におけるプライマリプロバイダを識別する。従って、新たにマ

ージプロバイダを定義する場合や、既存のマージプロバイダのプライマリプロバイダを他の認証プロバイダに変更する場合は、マージプロバイダ管理テーブル 192 を変更すればよく、マージプロバイダのソースコードを修正する必要はない。

【0038】

本実施の形態においては、パスワード・指紋マージプロバイダ 16 がマージプロバイダであるため、パスワード・指紋マージプロバイダ 16 に対応するレコードが登録されている。また、パスワード・指紋マージプロバイダ 16 のプライマリプロバイダは、上述したようにパスワード認証プロバイダ 17 であるため、パスワード・指紋マージプロバイダ 16 のプライマリプロバイダのプロバイダ名として、パスワード認証プロバイダ 17 のプロバイダ名が登録されている。

【0039】

また、図 4 は、マージ情報管理 DB を構成する追加プロバイダ管理テーブルの構成例を示す図である。図 3 の追加プロバイダ管理テーブル 193（第二の認証手段識別情報管理手段）は、各マージプロバイダに属する追加プロバイダを識別するためのテーブルであり、マージプロバイダ名及び追加プロバイダ名等のデータ項目を有する。マージプロバイダ名は、マージプロバイダのプロバイダ名である。追加プロバイダ名は、当該マージプロバイダにおいて追加プロバイダとなっているプロバイダ名である。

【0040】

本実施の形態においては、パスワード・指紋マージプロバイダ 16 の追加プロバイダは、指紋認証プロバイダ 18 であるため、その旨が追加プロバイダ管理テーブル 193 に登録されている。なお、パスワード・指紋マージプロバイダ 16 に更に追加プロバイダを追加する場合は、パスワード・指紋マージプロバイダ 16 のプロバイダ名をマージプロバイダ名とし、更に追加プロバイダとして登録する認証プロバイダのプロバイダ名を追加プロバイダ名とした新たなレコードを、追加プロバイダ管理テーブル 193 に登録すればよい。

【0041】

また、図 5 は、マージ情報管理 DB を構成する認証プロバイダマージテーブル

の構成例を示す図である。図5の認証プロバイダマージテーブル194（ユーザID対応管理手段）は、プライマリプロバイダにおけるユーザの識別情報（ユーザID等）と、追加プロバイダにおけるユーザIDとを対応づけるテーブルであり、マージプロバイダ名、プライマリID、追加プロバイダ名、及び追加ID等のデータ項目を有する。

【0042】

マージプロバイダ名は、マージプロバイダのプロバイダ名である。プライマリIDとは、プライマリプロバイダに対応する認証エンジンにおいて、各ユーザに一意に割り当てられたユーザIDである。追加プロバイダ名は、追加プロバイダのプロバイダ名である。追加プロバイダ名の項目は、上述したように一つのマージプロバイダに複数の追加プロバイダを登録することが可能なため、後述する追加IDがどの追加プロバイダにおけるものかを識別するために設けてあるものである。追加IDは、追加プロバイダ名によって識別される追加プロバイダに対応する認証エンジンにおいて、各ユーザに一意に割り当てられたユーザIDである。

【0043】

即ち、各ユーザを識別するためのコード体系は、各認証エンジンで異なるのが一般である。従って、それぞれの認証エンジンを有機的に連携させるためには、一方の認証エンジンにおけるユーザIDによって特定されるユーザの他方の認証エンジンにおけるユーザIDを特定するための手段が必要とされる。かかる手段を提供するのが認証プロバイダマージテーブル194である。なお、認証プロバイダマージテーブル194は、認証サービスモジュール11に対して一つ実装してもよいし、マージプロバイダ一つに対して一つ、即ちマージプロバイダが有するように実装してもよい。

【0044】

認証プロバイダ管理テーブル194について更に具体的に説明する。本実施の形態においては、パスワード・指紋マージプロバイダ16のプライマリプロバイダであるパスワード認証プロバイダ17は、上述したように外部認証サーバ40に対応する認証プロバイダである。ここで、外部認証サーバ40は、パスワード

認証を行う認証エンジンを実装したサーバであるため、例えば、図6に示されるユーザ管理テーブルを有している。

【0045】

図6は、外部認証サーバにおけるユーザ管理テーブルの構成例を示す図である。図6のユーザ管理テーブル41は、ユーザ毎に、ユーザID、パスワード、及び氏名等のユーザ情報を管理している。ここでユーザIDが、認証プロバイダマージテーブル194におけるプライマリIDに該当する。

【0046】

一方、パスワード・指紋マージプロバイダ16の追加プロバイダである指紋認証プロバイダ18は、上述したように、指紋認証ライブラリ181と指紋DB182による指紋認証エンジンに対応する認証プロバイダである。ここで、指紋DB182は、例えば、図7に示される指紋特徴データ管理テーブルを有している。

【0047】

図7は、指紋DBを構成する指紋特徴データ管理テーブルの構成例を示す図である。図7の指紋特徴データ管理テーブル1821は、ユーザIDと指紋特徴データとをデータ項目として有する。ユーザIDは、指紋特徴データを一意に識別するための識別情報である。指紋特徴データは、指紋特徴データの実体である。ここで、ユーザIDが、マージテーブル194における追加IDに該当する。

【0048】

従って、認証プロバイダマージテーブル194より、外部認証サーバ40においてユーザIDが0001のユーザの指紋特徴データを特定することが可能となる。また、ユーザIDの対応づけを認証プロバイダマージテーブル194によって管理することにより、ユーザIDの対応づけに変更がある場合においても容易に対応することができる。

【0049】

上述した、認証プロバイダ管理テーブル191、マージプロバイダ管理テーブル192、追加プロバイダ管理テーブル193、及び認証プロバイダマージテーブル194によって、マージプロバイダの動作に必要な情報が管理されることに

より、マージプロバイダのソースコードを汎用的なものとすることができる。即ち、唯一のソースコードから複数の異なるマージプロバイダを実現させることができる。

【0050】

図8は、本発明の実施の形態における認証サーバのハードウェア構成例を示す図である。図8の認証サーバ10は、それぞれバスBで相互に接続されているドライブ装置100と、補助記憶装置102と、メモリ装置103と、演算処理装置104と、インタフェース装置105とを有するように構成される。

【0051】

認証サーバ10において認証サービスモジュール11を実現するユーザ認証プログラムは、CD-ROM等の記憶媒体101によって提供される。ユーザ認証プログラムを記録した記憶媒体101は、ドライブ装置100にセットされると、ユーザ認証プログラムが記憶媒体101からドライブ装置100を介して補助記憶装置102にインストールされる。

【0052】

補助記憶装置102は、インストールされたユーザ認証プログラムを格納すると共に、必要なファイルやデータ等を格納する。例えば補助記憶装置102は、ユーザ認証プログラムの処理に必要な、上述した各種テーブルを格納している。

【0053】

メモリ装置103は、認証サーバ10の起動時等、ユーザ認証プログラムの起動指示があった場合に、補助記憶装置102からユーザ認証プログラムを読み出して格納する。演算処理装置104は、メモリ装置103に格納されたユーザ認証プログラムに従って認証サーバ10に係る機能を実行する。インタフェース装置105は例えばモデム、ルータ等で構成され、LAN又はインターネット等のネットワークに接続するために用いられる。

【0054】

以下、図1の認証サーバ10の処理手順について説明する。なお、以下の説明において、プライマリプロバイダを利用した認証を「プライマリ認証」と、追加プロバイダを利用した認証を「追加認証」という。図9は、プライマリ認証の際

の認証サーバの処理を説明するためのシーケンス図である。

【0055】

ユーザがクライアントアプリケーション23を利用すべくクライアントアプリケーション23を起動すると、クライアントアプリケーション23は、ユーザに対しユーザID及びパスワードの入力を要求する。ユーザがユーザID及びパスワードを入力すると、クライアントアプリケーション23は、プロバイダ呼び分け手段13が提供する認証関数（Authenticate（プロバイダ名、ドメイン名、ユーザID、パスワード））をSOAPのRPCで呼び出すことにより、認証サーバ10に対しユーザの認証を要求する（S11）。なお、認証関数の各引数の意味は以下の通りである。

【0056】

プロバイダ名は、認証に利用する認証プロバイダであるであり、ここではパスワード・指紋マージプロバイダ16のプロバイダが指定される。ドメイン名は端末20が属するドメインのドメイン名である。ユーザID以降は、認証に利用する認証プロバイダによって、指定する値が異なる。本実施の形態では、パスワード・指紋マージプロバイダ16のプライマリプロバイダは、パスワード認証プロバイダ17であるため、パスワード認証に必要な情報としてユーザに入力させたユーザIDとパスワードが指定される。

【0057】

ステップS11に続いてステップS12に進み、RPCによって認証関数が呼び出されたプロバイダ呼び分け手段13は、認証関数の引数のプロバイダ名によって指定されている認証プロバイダを呼び出すために必要な情報を認証プロバイダ管理テーブル191から取得し、当該認証プロバイダを呼び出す。ここでは、パスワード・指紋マージプロバイダ16が呼び出される。

【0058】

ステップS12に続いてステップS13に進みパスワード・指紋マージプロバイダ16は、自己のプライマリプロバイダとして登録されている認証プロバイダをマージプロバイダ管理テーブル192に基づいて識別し、当該プライマリプロバイダの認証関数（Authenticate（ドメイン名、ユーザID、パスワード））を

呼び出す。ここでは、パスワード認証プロバイダ 1 7 の認証関数呼び出される。
なお、プライマリプロバイダの認証関数の各引数の値は、ディパッチャ 1 3 の認証関数が呼び出される際に指定された値が引き継がれる。

【 0 0 5 9 】

ステップ S 1 3 に続いてステップ S 1 4 に進み、パスワード認証プロバイダ 1 7 は、外部認証サーバ 4 0 を利用してパスワード認証を実行する。ユーザが正当であることが確認されたらステップ S 1 5 に進み、パスワード認証プロバイダはチケットを生成する。

【 0 0 6 0 】

ここで、チケットについて説明する。本実施の形態におけるチケットとは、認証にパスしたユーザ（クライアント）に対して認証プロバイダが発行する、当該ユーザが認証されたことを証明する電子的な証明書をいう。チケットを発行されたクライアントは、文書管理サーバ等、所定のサーバを利用する際にチケットを提示することにより当該サーバを利用する権限を得ることができる。

【 0 0 6 1 】

図 1 0 は、通常のチケットのデータ構造の例を示す図である。図 1 0 に示されるようにチケット 5 0 1 は、チケット ID、有効範囲、認証プロバイダ名、有効期限、認証ドメイン名、認証ユーザ ID、主なユーザ属性のリスト、及び MIC 等から構成される。

【 0 0 6 2 】

チケット ID は、発行されたチケットを一意に識別するためのコードである。有効範囲については後述する。認証プロバイダ名は、実際に認証を行った（チケットを発行した）認証プロバイダのプロバイダ名である。有効期限は、当該チケットが有効な期限である。認証ドメイン名及び認証ユーザ ID は、認証を受けユーザに対応するドメイン名及びユーザ ID である。主なユーザ属性リストは、認証を受けたユーザの様々な属性（例えば、所属、役職等）である。MIC は、当該チケットが途中で改竄されていないかを確認するためのコードである。

【 0 0 6 3 】

なお、チケットには、認証チケットとマスタチケットとがある。認証チケット

とは、限られた範囲でのみ利用可能なチケットである。限られた範囲とは、所定のドメイン内でのみ利用可能であることや、所定のシステム又はサーバのみで利用可能であることを意味する。例えば、文書管理システムのみで利用可能な認証チケットは、他のシステムでは利用できない。従って、万が一認証チケットを盗まれた場合は、ユーザが受ける被害盗まれた認証チケットが有効な範囲のみに限られる。

【0064】

これに対し、マスタチケットとは、チケットに対応しているシステムの全範囲に渡って利用可能な万能のチケットである。認証チケットの発行を要求する際には、マスタチケットを提示する必要がある。但し、その万能性ゆえ、マスタチケットを盗まれた場合には、被害はチケットに対応しているシステムの全範囲に及ぶ可能性がある。従って、マスタチケットは、認証チケットの発行要求等、マスタチケットの提示が必須の場合のみ利用し、通常のサービスを受ける際には、認証チケットを利用するといった使い分けをすることにより、より高度なセキュリティを確保することができる。

【0065】

上記の説明において保留にした、チケットの構成要素である有効範囲は、かかる分類を識別するためのものである。即ち、当該チケットがマスタチケットである場合は、有効範囲には「マスタ」と記録され、認証チケットである場合は、当該認証チケットが有効な範囲を識別するための名称（ドメイン名、サーバ名等）が記録される。

【0066】

なお、図9において、ステップS11からステップS19まではマスタチケットを発行するための処理に係り、ステップS20からステップS29まではマスタチケットを提示して認証チケットを得るための処理に係る。

【0067】

また、別の観点から、チケットにはinnerチケットとouterチケットとがある。innerチケットとは、その名の通り内部のチケット、即ち、認証サーバ10の内部におけるチケットに対する呼び名である。これに対しout e

r チケットとは、認証管理サーバ 10 の外部におけるチケットに対する呼び名である。即ち、inner チケットと outer チケットとの違いは、記録されている情報の内容が異なるといった本質的なものではない。認証サーバ 10 から端末 20 等へチケットが送信される際等に、チケットは、inner チケットから outer チケットに変換される。一方、認証サーバ 10 が端末 20 等から outer チケットを受信した際には、チケットは、outer チケットから inner チケットへと変換される。ここで変換の具体例としては、暗号化が挙げられる。即ち、inner チケットを暗号化したものが outer チケットという関係である。チケットを暗号化することにより、例えばチケットが盗まれた場合でも、その内容が不正に利用されることを防止することができる。

【0068】

更に、本実施の形態においては、チケットをその発行元によって、プライマリチケットと追加チケットとに呼び分ける。プライマリチケットとは、プライマリプロバイダが発行したチケットをいい、追加チケットとは、追加プロバイダが発行したチケットをいう。

【0069】

ステップ S15 においてパスワード認証プロバイダ 17 は、inner 型のマスタチケットを生成する。また、パスワード認証プロバイダ 17 は、プライマリプロバイダであるため、生成したチケットはプライマリチケットに分類される。よって、以下、ステップ S15 においてパスワード認証プロバイダ 17 が生成したチケットを「マスタプライマリチケット」という。

【0070】

マスタプライマリチケットの各項目には以下のような値が記録されている。

【0071】

有効範囲：「マスタ」

認証プロバイダ名：「パスワード認証プロバイダ」

有効期限：2002/MM/DD

認証ドメイン名：＜認証関数の引数に指定されたドメイン名＞

認証ユーザ ID：＜認証関数の引数に指定されたユーザ ID＞

ステップS 15に続いてステップS 16に進み、パスワード認証プロバイダ17は、認証関数の戻り値として、生成したマスタプライマリチケットをパスワード・指紋マージプロバイダ16に出力する。ステップS 16に続いてステップS 17に進み、パスワード・指紋マージプロバイダ16は、マージ (Merge) チケットを生成し、マージチケットにマスタプライマリチケットをマージする。

【0072】

図11は、マージチケットのデータ構造の例を示す図である。図11に示されるマージチケット502は、複数のチケットをマージするためのチケットであり、チケット種別、認証プロバイダ名、有効期限、プライマリプロバイダ名、プライマリチケット、追加チケットのリスト、及びMIC等から構成される。

【0073】

チケット種別は、図10に示される通常のチケット501における「有効範囲」と同義である。認証プロバイダ名は、当該マージチケットを発行した認証プロバイダ名である。従って、ここでは認証プロバイダ名にはパスワード・指紋マージプロバイダ16のプロバイダ名が記録される。有効期限は、当該マージチケットの有効期限である。プライマリプロバイダ名は、当該マージチケットにマージされたプライマリチケットを発行したプライマリプロバイダのプロバイダ名である。従って、ここではパスワード認証プロバイダ16のプロバイダ名が記録される。プライマリチケットは、プライマリプロバイダが発行した、プライマリチケットそのものが記録される。従って、ここではパスワード認証プロバイダ16が発行したマスタプライマリチケットが記録される。追加チケットのリストは、追加プロバイダの発行する追加チケットが記録される。但し、この時点では、まだ追加プロバイダによる認証は実行されていないため、追加チケットのリストは空である。MICは、通常のチケット501におけるMICと同義である。

【0074】

なお、マージチケットについても、マスタチケット／認証チケットの区別と、innerチケット／outerチケットの区別とがあるが、ステップS 17で生成されるのは、inner型でかつマスタ型のマージチケットである。従って、ステップS 17においゑパスワード・指紋マージプロバイダ16が生成したチ

ケットを、以下「マスタマージチケット」という。

【0075】

ステップS17に続いてステップS18に進み、パスワード・指紋マージプロバイダ16は、生成したマスタマージチケットをプロバイダ呼び分け手段13に対して出力する。ステップS18に続いてステップS19に進み、プロバイダ呼び分け手段13は、inner型のマスタマージチケットをouter型に変換（例えば暗号化）し、outer型に変換されたマスタマージチケットをクライアントアプリケーション23に送信する。

【0076】

ステップS19が完了した時点で、クライアントアプリケーション23は、マスタマージチケットを取得したことになる。上述したようにマスタチケットは、万能のチケットであるため、このままマスタマージチケットを利用して他のシステムを利用することも可能であるが、マスタチケットをネットワーク上に頻繁に流通させるのは、セキュリティ上好ましくない。従って、クライアントアプリケーション23は、プロバイダ呼び分け手段13の認証チケット生成関数（create AuthTicket（マスタマージチケット））をSOAPのRPCで呼び出すことにより、利用対象とするシステムに対してのみ有効な認証チケットの生成を認証サーバ10に要求する（S20）。なお、認証チケット生成関数の引数には、ステップS19で取得した、outer型のマスタマージチケットを指定する。

【0077】

ステップS20に続いてステップS21に進み、認証チケット生成関数が呼び出されたプロバイダ呼び分け手段13は、outer型のマスタマージチケットをinner型に変換（暗号化を解除）する。更に、プロバイダ呼び分け手段13は、マスタマージチケットの「認証プロバイダ名」を確認することにより、マスタマージチケットを発行した認証プロバイダを判別する。

【0078】

ステップS21に続いてステップS22に進み、プロバイダ呼び分け手段13は、マスタマージチケットの発行元である認証プロバイダを呼び出す。従って、ここではパスワード・指紋マージプロバイダ16が呼び出される。ステップS2

2に続いてステップS 2 3に進み、パスワード・指紋マージプロバイダ1 6は、マスタマージチケットの正当性を有効期限及びM I C等により確認する。

【0079】

ステップS 2 3に続いてステップS 2 4に進み、パスワード・指紋マージプロバイダ1 6は、マスタマージチケットにマージされているプライマリチケットを発行したプライマリプロバイダの認証チケット生成関数（createAuthTicket（マスタプライマリチケット））を呼び出す。従って、ここではパスワード認証プロバイダ1 7の認証チケット生成関数が呼び出される。なお、パスワード認証プロバイダ1 7の認証チケット生成関数の引数には、マスタマージチケットから取り出したマスタプライマリチケットが指定される。

【0080】

ステップS 2 4に続いてステップS 2 5に進み、パスワード認証プロバイダ1 7は、引数に指定されたマスタプライマリチケットの正当性を有効期限及びM I C等により確認し、認証チケットを生成する。認証チケットのデータ構造は、図1 0において説明した通りであり、マスタプライマリチケットと同様に各項目に値が記録される。但し、「有効範囲」については、マスタプライマリチケットと異なり、当該認証チケットが有効なサーバ名又はドメイン名等が記録される。

【0081】

なお、ここで生成された認証チケットについても、プライマリプロバイダであるパスワード認証プロバイダ1 7が生成したものであるという意味で、プライマリチケットに分類される。従って、以下、ステップS 2 5においてパスワード認証プロバイダ1 7が生成した認証チケットを「認証プライマリチケット」という。

【0082】

ステップS 2 5に続いてステップS 2 6に進み、パスワード認証プロバイダ1 7は、認証チケット生成関数の戻り値として、生成した認証プライマリチケットをパスワード・指紋マージプロバイダ1 6に出力する。ステップS 2 6に続いてステップS 2 7に進み、パスワード・指紋マージプロバイダ1 6は、マージチケットを生成し、マージチケットに認証プライマリチケットをマージする。

【0083】

ここで、パスワード・指紋マージプロバイダ16が生成するマージチケットは、有効範囲が限定された認証チケットである。よって、ステップS27においてパスワード・指紋マージプロバイダ16が生成したマージチケットを、以下「認証マージチケット」という。

【0084】

ステップS27に続いてステップS28に進み、パスワード・指紋マージプロバイダ16は、生成した認証マージチケットをプロバイダ呼び分け手段13に対して出力する。ステップS28に続いてステップS29に進み、プロバイダ呼び分け手段13は、inner型の認証マージチケットをouter型に変換し、outer型に変換された認証マージチケットをクライアントアプリケーション23に送信する。

【0085】

以上により、クライアントアプリケーション23は、マスタマージチケットに次いで認証マージチケットを取得したことになる。従って、クライアントアプリケーション23は、認証マージチケットの有効なサーバに対して認証マージチケットを提示することにより、当該サーバのサービスを利用することができる。但し、上記においては、プライマリプロバイダ（パスワード認証プロバイダ17）による認証しか受けていないため、クライアントアプリケーション23に与えられた権限は、プライマリプロバイダによって認証を受けた範囲に限られる。

【0086】

ここでいう「認証を受けた範囲」における「範囲」とは、チケット501のデータ項目である「有効範囲」における「範囲」と異なる概念である。「有効範囲」における範囲は、例えば、当該チケットは、サーバAとサーバBとで有効であるというように、利用可能な対象を示す意味での範囲である。一方、「認証を受けた範囲」における範囲は、当該チケットは、プライマリプロバイダのみに認証を受けており、追加プロバイダには認証されていないといったように、認証を受けたレベルを示すものである。たとえていえば、前者は平面的な広がりにおける範囲をいい、後者は深さ方向における範囲をいう。

【0087】

以下、ユーザが、更に”深い”、即ち、本人であることを更に保障するための追加認証を受ける際の処理について説明する。図12及び図13は、追加認証の際の認証サーバの処理を説明するためのシーケンス図である。クライアントアプリケーション23のユーザが、パスワード認証プロバイダ17によって認証を受けただけでは、利用できないサービスを利用しようとした場合を想定する。例えば、重要な機密情報にアクセスしようとした場合、又は、部下の承認要求に対し承認を実行しようとした場合などがいい例である。ユーザがかかる処理要求を行った場合に、本実施の形態におけるクライアントアプリケーション23は、ユーザに対し指紋の入力を要求する。

【0088】

但し、ここではユーザIDの入力は必要とされない。一般に、認証を受ける際には、ユーザID等のユーザを一意に特定するための情報ユーザと、パスワード、指紋等のユーザが本人であることを保証するための情報を入力が必要である。ユーザIDの入力のみでは、ユーザが本人であるかを判断することができず、パスワードや指紋の入力のみでは、誰のパスワード又は指紋であるのか判断することができないからである。従って、通常であれば、ここにおいて、ユーザは指紋と共に、ユーザIDの入力が要求されるはずである。しかし、本実施の形態におけるパスワード・指紋マージプロバイダ16は、詳細については後述されるが、既にプライマリ認証の際に入力されたユーザID（プライマリID）に基づいて、当該ユーザの追加認証におけるユーザID（追加ID）を特定するため、ユーザに、追加認証の際にユーザIDの入力を要求する必要がないのである。

【0089】

ユーザが指紋読み取りデバイス25に指紋を読み取らせると、クライアントアプリケーション23は、プロバイダ呼び分け手段13の追加認証関数（authenticate（マスタマージチケット、追加認証プロバイダ名、指紋特徴データ）をSOAPのRPCによって呼び出すことにより、認証サーバ10に対して追加認証を要求する（S41）。

【0090】

なお、追加認証関数の引数の意味は、以下の通りである。マスタマージチケットには、マスタプライマリチケットがマージされている既に取得済みのマスタマージチケットを指定する。追加認証プロバイダ名には、追加認証を要求する追加プロバイダのプロバイダ名を指定する。従って、ここでは指紋認証プロバイダ 18 のプロバイダ名を指定する。指紋特徴データには、指紋読み取りデバイス 25 で読み取った指紋特徴データを指定する。

【0091】

ステップ S 4 1 に続いてステップ S 4 2 に進み、追加認証関数が呼び出されたプロバイダ呼び分け手段 13 は、マスタマージチケットの「認証プロバイダ名」を確認することにより、マスタマージチケットを発行した認証プロバイダを判別する。なお、本ステップ以降の説明においては、チケットについての outer 形、inner 型の区別については省略する。

【0092】

ステップ S 4 2 に続いてステップ S 4 3 に進み、プロバイダ呼び分け手段 13 は、マスタマージチケットの発行元である認証プロバイダを呼び出す。従って、ここではパスワード・指紋マージプロバイダ 16 が呼び出される。ステップ S 4 3 に続いてステップ S 4 4 に進み、パスワード・指紋マージプロバイダ 16 が、マスタマージチケットからマスタプライマリチケットを取り出し、マスタプライマリチケットの所有者であるユーザのユーザ ID（プライマリ ID）の取得をプライマリプロバイダであるパスワード認証プロバイダ 17 に要求すると、パスワード認証プロバイダ 17 は、マスタプライマリチケットの正当性を確認すると共に、マスタプライマリチケットから認証ユーザ ID を取り出し、パスワード・指紋マージプロバイダ 16 に対して取り出した認証ユーザ ID をプライマリ ID として出力する。

【0093】

ステップ S 4 4 に続いてステップ S 4 5 に進み、パスワード・指紋マージプロバイダ 16 は、パスワード認証プロバイダ 17 から取得したプライマリ ID をキーとして、認証プロバイダマージテーブル 194 を検索し、プライマリ ID に対応する追加 ID を取得する。なお、ここで取得された追加 ID は、指紋 DB 18

2の指紋特徴データ管理テーブル1821におけるユーザIDに該当する。

【0094】

ステップS45に続いてステップS46に進み、パスワード・指紋マージプロバイダ16は、追加認証関数の引数で指定された追加認証プロバイダ名によって特定される追加プロバイダの認証関数（Authenticate（追加ID、指紋特徴データ））を呼び出す。従って、ここでは指紋認証プロバイダ18の認証関数が呼び出される。

【0095】

ステップS46に続いてステップS47に進み、認証関数が呼び出された指紋認証プロバイダ18は、引数に指定された追加ID（ユーザID）をキーに指紋DB182から指紋特徴データを取り出し、取り出した指紋特徴データと、認証関数の引数に指定された指紋特徴データとを照合する。

【0096】

ここで、認証関数の引数に指定された指紋特徴データは、追加認証を要求したユーザのものである。一方、ステップS47において指紋DB182から取り出された指紋特徴データは、プライマリ認証を受けたユーザのユーザIDであるプライマリIDをキーとして認証プロバイダマージテーブル194から検索した追加IDに対応するものである。

【0097】

従って、二つの指紋特徴データが一致することにより、追加認証を要求したユーザが、指紋DB182登録されているユーザであることと共に、プライマリ認証を受けたユーザと追加認証を受けたユーザとが同一人物であることが保証される。

【0098】

また、二つの認証をパスしたことで、クライアントアプリケーション23のユーザが本人であることの保証がより高まったといえる。

【0099】

従って、指紋認証プロバイダ18は、自らが認証したことを証明するマスタチケットを生成する（S48）。なお、指紋認証プロバイダ18は、追加プロバイ

ダであるため、指紋認証プロバイダ 18 が発行するチケットは追加チケットであるといえる。よって、ステップ S 48 において指紋認証プロバイダ 18 が生成したマスタチケットを、以下「マスタ追加チケット」という。

【0100】

なお、ここで生成されたマスタ追加チケットの「認証プロバイダ名」には、指紋認証プロバイダ 18 の認証プロバイダ名が記録され、認証ユーザ ID には、指紋 DB 182 におけるユーザ ID が記録される。

【0101】

ステップ S 48 に続いてステップ S 49 に進み、指紋認証プロバイダ 18 は、生成したマスタ追加チケットをパスワード・指紋マージプロバイダ 16 に出力する。ステップ S 49 に続いてステップ S 50 に進み、パスワード・指紋マージプロバイダ 16 は、既にマスタプライマリチケットがマージされているマスタマージチケットにマスタ追加チケットをマージする。

【0102】

ステップ S 50 に続いてステップ S 51 に進み、パスワード・指紋マージプロバイダ 16 は、マスタ追加チケットを更にマージしたマスタマージチケットをプロバイダ呼び分け手段 13 に出力する。ステップ S 51 に続いてステップ S 52 に進み、プロバイダ呼び分け手段 13 は、クライアントアプリケーション 23 に対してマスタマージチケットを送信する。この時点でクライアントアプリケーション 23 は、追加チケットがマージされた（追加認証を受けた）更に信頼性の高いマスタマージチケットを入手したことになる。

【0103】

ステップ S 52 に続いて図 13 のステップ S 53 に進み、以降は図 9 のステップ S 20 以降の処理と同様に、クライアントアプリケーション 23 が認証チケットを取得するための処理である。従って、ステップ S 53 からステップ S 59 までは、図 9 のステップ S 20 からステップ S 26 までの処理と同様である。即ち、クライアントアプリケーション 23 によるプロバイダ呼び分け手段 13 の認証チケット生成関数（createAuthTicket（マスタマージチケット））の呼び出しに基づいて（S 53）、パスワード認証プロバイダ 17 によって認証プライマリチ

ケットが生成され、パスワード・指紋マージプロバイダ16に出力される（S54～S59）。

【0104】

ここで、認証プライマリチケットを受け取ったパスワード・指紋マージプロバイダ16は、マスタマージチケットが追加認証されたものであるのか、即ち、マスタマージチケットにマスタ追加チケットがマージされているか否かを判断する。

【0105】

マスタマージチケットにマスタ追加チケットがマージされていない場合は、図9の場合と同様に認証プライマリチケットがマージされた認証マージチケットがクライアントアプリケーション23に送信される（S60）。しかし、今回は、既にマスタマージチケットについて追加認証を受けている。従って、パスワード・指紋マージプロバイダ16は、追加プロバイダからも認証チケットを取得するため、マスタマージチケットにマージされている追加チケットを発行した追加プロバイダの認証チケット生成関数（createAuthTicket（マスタ追加チケット））を呼び出す（S61）。従って、ここでは指紋認証プロバイダ18の認証チケット生成関数が呼び出される。なお、指紋認証プロバイダ18の認証チケット生成関数の引数には、マージチケットから取り出したマスタ追加チケットが指定される。

【0106】

ステップS61に続いてステップS62に進み、指紋認証プロバイダ18は、引数に指定されたマスタ追加チケットの正当性を有効期限及びMIC等により確認し、正当である場合は、認証チケット（以下、「認証追加チケット」という。）を生成する。

【0107】

ステップS62に続いてステップS63に進み、指紋認証プロバイダ18は、認証チケット生成関数の戻り値として、生成した認証追加チケットをパスワード・指紋マージプロバイダ16に出力する。ステップS63に続いてステップS64に進み、パスワード・指紋マージプロバイダ16は、認証マージチケットを生

成し、ステップ S 5 9 で取得した認証プライマリチケットと、ステップ S 6 3 で取得した認証追加チケットとを認証マージチケットにマージする。

【0108】

ステップ S 6 4 に続いてステップ S 6 5 に進み、以降、認証マージチケットがクライアントアプリケーション 2 3 に送信される (S 6 6)。

【0109】

以上により、クライアントアプリケーション 2 3 は、図 9 のステップ S 2 9 において入手した認証マージチケットよりも信頼性が高い、追加認証された認証マージチケットを取得したことになる。従って、クライアントアプリケーション 2 3 は、認証マージチケットの有効なサーバに対して認証マージチケットを提示することにより、更にセキュリティレベルの高いサービスを利用することができる。

【0110】

なお、図 1 2 のステップ S 4 1 においてクライアントアプリケーション 2 3 が呼び出すプロバイダ呼び分け手段 1 3 の追加認証関数 (addAuthenticate) は、引数として追加認証プロバイダ名の指定を要求している。これは、クライアント主導で次に追加認証を行わせる追加プロバイダが決定されることを示している。

【0111】

即ち、上述においては、パスワード・指紋マージプロバイダ 1 6 の追加プロバイダとして指紋認証プロバイダ 1 8 一つのみが定義されている例について説明したが、追加プロバイダ管理テーブル 1 9 3 と認証プロバイダマージテーブル 1 9 4 に新たな認証プロバイダの情報を追加すれば、パスワード・指紋マージプロバイダ 1 6 に複数の追加プロバイダを定義することも可能である。

【0112】

かかる追加プロバイダが複数ある場合に、上述の例では、追加認証を行わせる追加プロバイダの順番は、追加認証関数を呼び出すクライアントの指定に従うことになる。

【0113】

しかし、追加認証を行わせる追加プロバイダの順番は、マージプロバイダ (パ

スワード・指紋マージプロバイダ 16) に判断させるようにしてもよい。例えば、追加プロバイダ管理テーブル 193 に新たなデータ項目として「順番」を追加し、「順番」項目に追加認証を行わせる順番を登録しておく。クライアントアプリケーション 23 から追加認証の要求があった場合は、マージプロバイダが追加プロバイダ管理テーブル 193 の「順番」項目を確認することにより、次に呼び出す追加プロバイダを決定する。

【0114】

この場合は、追加認証関数の引数から追加プロバイダ名を削除してしまってもよいし、そのまま指定させるようにしてもよい。そのまま指定させるようにした場合は、追加認証関数の引数に指定された追加プロバイダ名と、マージプロバイダが判断した追加プロバイダ名とを比較することにより、サーバ側とクライアント側とのフェーズが一致しているか否かを確認することができる。

【0115】

次に、認証サーバ 10 が発行したチケットがどのように利用されるかについて説明する。図 14 は、チケットの第一の利用方法を説明するためのシーケンス図である。図 14 において、クライアント 30 は、クライアントアプリケーション 23 でもよいが、ここでは、クライアントアプリケーション 23 等に所定のサービスを提供するサーバであるとする。そして、クライアント 30 がクライアントアプリケーション 23 からサービスの利用要求と共に認証マージチケットの提示を受けた場合を想定する。なお、クライアント 30 は、クライアントアプリケーション 23 に対してはサーバであるが、認証サーバ 30 に対しては「クライアント」であるため、図 14 においてクライアント 30 と表現している。

【0116】

認証マージチケットの提示を受けたクライアント 30 は、自分自身ではチケットの中身を解釈することができない。クライアントアプリケーション 23 から提示された認証マージチケットは暗号化 (outer 型) されており、また、クライアント 30 は、チケットの構造については関知しないからである。

【0117】

よって、クライアント 30 は、ステップ S101 において、プロバイダ呼び分

け手段13の提供するチケット解読関数（decodeTicket（認証マージチケット））を呼び出すことにより、認証マージチケットの解読を認証サーバ10に要求する。なお、チケット解読関数の引数には、クライアントアプリケーション23から提示（送信）された認証マージチケットを指定する。

【0118】

ステップS101に続いてステップS102に進み、チケット解読関数が呼び出されたプロバイダ呼び分け手段13は、認証マージチケットを発行した認証プロバイダを判別する。

【0119】

ステップS102に続いてステップS103に進み、プロバイダ呼び分け手段13は、認証マージチケットの発行元であるパスワード・指紋マージプロバイダ16を呼び出す。ステップS103に続いてステップS104に進み、パスワード・指紋マージプロバイダ16は、認証マージチケットの正当性を有効期限及びMIC等により確認し、認証マージチケットにマージされているプライマリチケットを発行したパスワード認証プロバイダ17のチケット解読関数（decodeTicket（認証プライマリチケット））を呼び出す（S105）。なお、パスワード認証プロバイダ17のチケット解読関数の引数には、認証マージチケットから取り出した認証プライマリチケットが指定される。

【0120】

ステップS105に続いてステップS106に進み、パスワード認証プロバイダ17は、引数に指定された認証プライマリチケットの正当性を有効期限及びMIC等により確認するとともに認証プライマリチケットの内容を解釈し、プライマリチケットの内容をクライアント30が解釈可能な形式、例えばテキスト形式にした認証情報データ（以下、「プライマリ認証情報データ」という。）を生成する。

【0121】

ステップS106に続いてステップS107に進み、パスワード認証プロバイダ17は、生成したプライマリ認証情報データをパスワード・指紋マージプロバイダ16に出力する。ここで、プライマリ認証情報データを受け取ったパスワー

ド・指紋マージプロバイダ16は、認証マスタマージチケットが追加認証されたものであるのかを判断する。追加認証されていない場合は、認証マスタマージチケットにはこれ以上認証情報は含まれていないため、プライマリ認証情報データがクライアント30に送信される（S108）。

【0122】

一方、既に認証マージチケットについて追加認証を受けている場合は、パスワード・指紋マージプロバイダ16は、認証マージチケットにマージされている追加チケットを発行した指紋認証プロバイダ18からも認証情報データを取得するため、指紋認証プロバイダ18のチケット解読関数（decodeTicket（認証追加チケット））を呼び出す（S109）。

【0123】

ステップS109に続いてステップS110に進み、指紋認証プロバイダ18は、引数に指定された認証追加チケットの正当性を有効期限及びMIC等により確認するとともに認証追加チケットの内容を解釈し、認証情報データ（以下、「追加認証情報データ」という。）を生成する。

【0124】

ステップS110に続いてステップS111に進み、指紋認証プロバイダ18は、生成した追加認証情報データをパスワード・指紋マージプロバイダ16に出力する。ステップS111に続いてステップS112に進み、パスワード・指紋マージプロバイダ16は、パスワード認証プロバイダ17から取得した追加認証情報データと、指紋認証プロバイダ18から取得した追加認証情報データとをマージする（以下、マージされた認証情報データを「マージ認証情報データ」という。）。

【0125】

図15は、マージ認証情報データの構成例を示す図である。例えば、マージ認証情報データは、図15に示されるように、認証サービス名、有効期限、有効範囲、認証プロバイダ、ユーザ識別子、所属グループ、及び主要属性等から構成される。

【0126】

認証サービス名は、認証サービスモジュール 11 に付けられた名前である。有効期限は、マージチケットに記録されている有効期限である。有効範囲は、プライマリチケット及び追加チケットに記録されている有効範囲をマージしたものである。即ち、「サーバA」と「サーバB」とがカンマで区切られているが、これは、プライマリチケットはサーバAで有効であり、追加チケットはサーバBで有効であることを示している。

【0127】

認証プロバイダは、チケットを発行した認証プロバイダの名前の羅列である。「パスワード認証プロバイダ」と「指紋認証プロバイダ」がカンマで区切られているが、これは、パスワード認証プロバイダ 17 と指紋認証プロバイダ 18 に認証を受けていることを示している。ユーザ識別子は、チケットの発行を受けたユーザを一意に識別するための情報である。所属グループ及び主要属性は、プライマリチケット及び追加チケットの「主なユーザ属性リスト」から抽出した情報をマージしたものである。

【0128】

ステップ S112 に続いてステップ S113 に進み、マージ認証情報データがクライアント 30 に送信される (S114)。

【0129】

以降、クライアント 30 は、取得したマージ認証情報データを確認することにより、クライアントアプリケーション 23 のユーザに対して提供可能なサービスを判断することができる。

【0130】

更に、図 16 は、チケットの第二の利用方法を説明するためのシーケンス図である。図 14 においては、クライアント 30 がチケットの解読結果を認証情報データとして受け取る例について説明したが、図 16 においては、チケットの正当性の確認と、チケットが誰に認証されたのか、あるいはどの程度まで（プライマリ認証まで、又は追加認証まで）認証されているのかを問い合わせる例について説明する。なお、図 16 におけるクライアント 30 の位置づけは、図 14 におけるそれと同じである。

【0131】

ステップS121においてクライアント30は、プロバイダ呼び分け手段13の提供するチケット確認関数（ValidateTicket（認証マージチケット））を呼び出すことにより、認証マージチケットの正当性の確認等を認証サーバ10に要求する。なお、チケット確認関数の引数には、クライアントアプリケーション23から提示（送信）された認証マージチケットを指定する。

【0132】

ステップS121に続いてステップS122に進み、チケット確認関数が呼び出されたプロバイダ呼び分け手段13は、認証マージチケットを発行した認証プロバイダを判別する。

【0133】

ステップS122に続いてステップS123に進み、プロバイダ呼び分け手段13は、認証マージチケットの発行元であるパスワード・指紋マージプロバイダ16を呼び出す。ステップS123に続いてステップS124に進み、パスワード・指紋マージプロバイダ16は、認証マージチケットの正当性を有効期限及びMIC等により確認し、認証マージチケットにマージされているプライマリチケットを発行したパスワード認証プロバイダ17のチケット確認関数（ValidateTicket（認証プライマリチケット））を呼び出す（S125）。なお、パスワード認証プロバイダ17のチケット確認関数の引数には、マージチケットから取り出した認証プライマリチケットが指定される。

【0134】

ステップS125に続いてステップS126に進み、パスワード認証プロバイダ17は、引数に指定された認証プライマリチケットの正当性を有効期限及びMIC等により確認し、確認結果をパスワード・指紋マージプロバイダ16に出力する（S127）。ここで確認結果とは、例えば、TRUEの場合は正当であり、FALSEの場合は不正であるといったBOOL値などでも良い。

【0135】

続いて、パスワード・指紋マージプロバイダ16は、認証マスタマージチケットが追加認証されたものであるのかを判断する。追加認証されていなければ、確

認結果がクライアント 30 に送信される (S 1 2 8)。ここでの確認結果とは、例えば、認証を行った認証プロバイダのプロバイダ名の羅列でもよいし、プライマリプロバイダまでは認証されているといったように、レベルを示すものでもよい。

【0136】

一方、既に認証チケットについて追加認証を受けている場合は、パスワード・指紋マージプロバイダ 16 は、認証マージチケットにマージされている追加チケットを発行した指紋認証プロバイダ 18 に対してもチケットの確認を依頼するため、指紋認証プロバイダ 18 のチケット確認関数 (ValidateTicket (認証追加チケット)) を呼び出す (S 1 2 9)。

【0137】

ステップ S 1 2 9 に続いてステップ S 1 3 0 に進み、指紋認証プロバイダ 18 は、引数に指定された認証追加チケットの正当性を有効期限及びMIC等により確認し、確認結果 (例えばBOOL値) をパスワード・指紋マージプロバイダ 16 に出力する (S 1 3 1)。ステップ S 1 3 1 に続いてステップ S 1 3 2 に進み、パスワード・指紋マージプロバイダ 16 は、パスワード認証プロバイダ 17 と指紋認証プロバイダ 18 とから取得した確認結果をマージしたものをクライアント 30 に対する確認結果としてプロバイダ呼び分け手段 13 に出力する。例えば、ここでの確認結果とは、認証を行った認証プロバイダのプロバイダ名の羅列でもよいし、追加プロバイダまでは認証されているといったように、レベルを示すものでもよい。

【0138】

ステップ S 1 3 2 に続いてステップ S 1 3 3 に進み、プロバイダ呼び分け手段 13 は、確認結果をクライアント 30 に送信する。

【0139】

確認結果を受信したクライアント 30、確認結果に基づいて、クライアントアプリケーション 23 のユーザに対して提供可能なサービスを判断することができる。

【0140】

上述したように、本実施の形態における認証サーバ10によれば、マージプロバイダが、認証プロバイダマージテーブル194によって、プライマリIDから追加IDを導出し、かかる追加IDに基づいて追加認証をおこなうため、プライマリ認証を受けたユーザと追加認証を受けようとしているユーザの同一性を保証し、当該ユーザが本人であることの保証をより高めることができる認証サービスを提供することができる。

【0141】

また、認証した結果は、チケットとして発行され、当該チケットは、有効範囲、有効期限、改竄チェック用のコードを有しているため、より高度なセキュリティを確保することができる。即ち、有効範囲で、利用可能なシステム等が制限され、有効期限によって、利用可能な期間が制限され、改竄チェック用のコードによって、チケットの正当性が担保されるからである。

【0142】

また、プライマリプロバイダや追加プロバイダが発行したチケットは、マージプロバイダによってマージチケットにマージされて発行されるため、チケットを発行された側は、各チケットの関連付けについて関与する必要はなく、チケットの取り扱いを容易にすることができる。

【0143】

なお、本実施の形態においては、認証サービスモジュール11が、ネットワークを介して接続されている端末20に配置されているクライアントアプリケーション23に対して認証機能を提供する例について説明したが、本発明は、かかるクライアント・サーバ型のシステムに限定されるものではない。

【0144】

図17は、内部アプリケーションに認証機能を提供する場合の認証サーバの機能構成例を示す図である。図17中、図1と同一部分には同一符号を付し、その説明は省略する。図17においては、アプリケーション41、42、43、及び44が、SOAP経由ではなく、プロバイダ呼び分け手段13の関数を直接呼び出すように構成されている。このように、認証サーバ10の内部に構築したアプリケーションからも、認証サービスモジュール11を利用することができる。

【0145】

以上、本発明の好ましい実施例について詳述したが、本発明は係る特定の実施形態に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

【0146】**【発明の効果】**

上述の如く、本発明によれば、ユーザの同一性を保証しつつ複数の認証機能によってユーザを認証することができる。

【図面の簡単な説明】**【図1】**

本発明の実施の形態における認証システムの構成例を示す図である。

【図2】

マージ情報管理DBを構成する認証プロバイダ管理テーブルの構成例を示す図である。

【図3】

マージ情報管理DBを構成するマージプロバイダ管理テーブルの構成例を示す図である。

【図4】

マージ情報管理DBを構成する追加プロバイダ管理テーブルの構成例を示す図である。

【図5】

マージ情報管理DBを構成する認証プロバイダマージテーブルの構成例を示す図である。

【図6】

外部認証サーバにおけるユーザ管理テーブルの構成例を示す図である。

【図7】

指紋DBを構成する指紋特徴データ管理テーブルの構成例を示す図である。

【図8】

本発明の実施の形態における認証サーバのハードウェア構成例を示す図である

。

【図 9】

プライマリ認証の際の認証サーバの処理を説明するためのシーケンス図である

。

【図 10】

通常のチケットのデータ構造の例を示す図である。

【図 11】

マージチケットのデータ構造の例を示す図である。

【図 12】

追加認証の際の認証サーバの処理を説明するためのシーケンス図である。

【図 13】

追加認証の際の認証サーバの処理を説明するためのシーケンス図である。

【図 14】

チケットの第一の利用方法を説明するためのシーケンス図である。

【図 15】

マージ認証情報データの構成例を示す図である。

【図 16】

チケットの第二の利用方法を説明するためのシーケンス図である。

【図 17】

内部アプリケーションに認証機能を提供する場合の認証サーバの機能構成例を示す図である。

【符号の説明】

- 1 認証システム
- 10 認証サーバ
- 11 認証サービスモジュール
- 12 SOAPスタブ
- 13 プロバイダ呼び分け手段
- 14 認証プロバイダA
- 15 認証プロバイダB

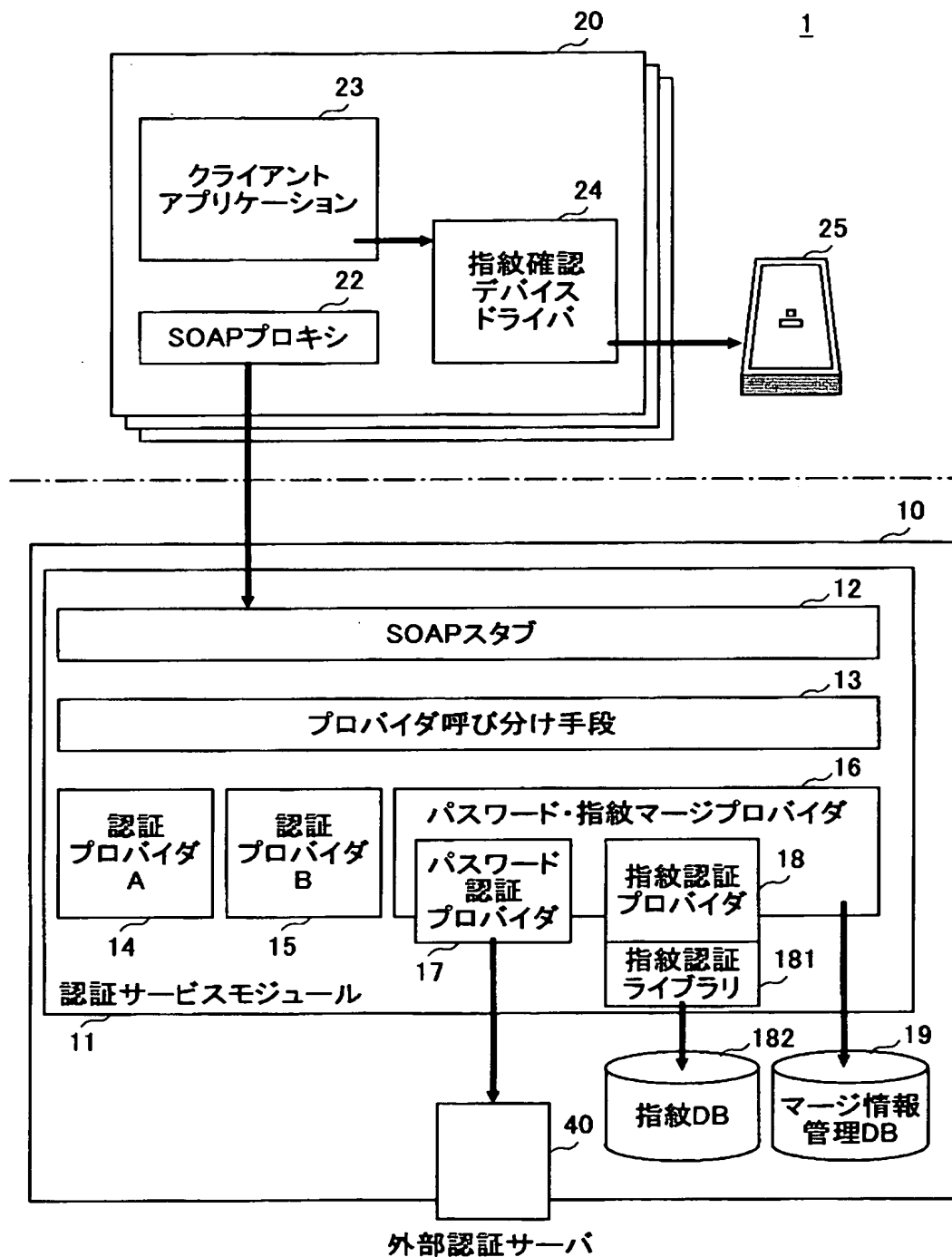
- 16 パスワード・指紋マージプロバイダ
- 17 パスワード認証プロバイダ
- 18 指紋認証プロバイダ
- 19 マージ情報管理DB
- 20 端末
- 22 SOAPプロキシ
- 23 クライアントアプリケーション
- 24 指紋読み取り装置ドライバ
- 25 指紋読み取り装置
- 40 外部認証サーバ
- 100 ドライブ装置
- 101 記憶媒体
- 102 補助記憶装置
- 103 メモリ装置
- 104 演算処理装置
- 105 インタフェース装置
- 181 指紋認証ライブラリ
- 182 指紋DB
- B バス

【書類名】

図面

【図 1】

本発明の実施の形態における認証システムの構成例を示す図



【図 2】

マージ情報管理DBを構成する
認証プロバイダ管理テーブルの構成例を示す図

191

プロバイダ名	実装名	実装依存の初期化情報
認証プロバイダA
認証プロバイダB
パスワード・指紋マージプロバイダ
パスワード認証プロバイダ
指紋認証プロバイダ

【図 3】

マージ情報管理DBを構成する
マージプロバイダ管理テーブルの構成例を示す図

マージプロバイダ名	プライマリプロバイダ名	
	パスワード・指紋マージプロバイダ	
	パスワード認証プロバイダ	

192

【図 4】

マージ情報管理DBを構成する
追加プロバイダ管理テーブルの構成例を示す図

193

マージプロバイダ名	追加プロバイダ名
パスワード・指紋マージプロバイダ	指紋認証プロバイダ

【図 5】

マージ情報管理DBを構成する
認証プロバイダマージテーブルの構成例を示す図

194

マージプロバイダ名	プライマリID	追加プロバイダ名	追加ID
パスワード・指紋マージプロバイダ	0001	指紋認証プロバイダ	5551
パスワード・指紋マージプロバイダ	0002	指紋認証プロバイダ	5552
パスワード・指紋マージプロバイダ	0003	指紋認証プロバイダ	5553
：	：	：	：

【図 6】

外部認証サーバにおけるユーザ管理テーブルの構成例を示す図

41

ユーザID	パスワード	氏名	...
0001	*****	XXXXXX	..
0002	*****	YYYYYY	..
0003	*****	ZZZZZZZZ	..
..

【図 7】

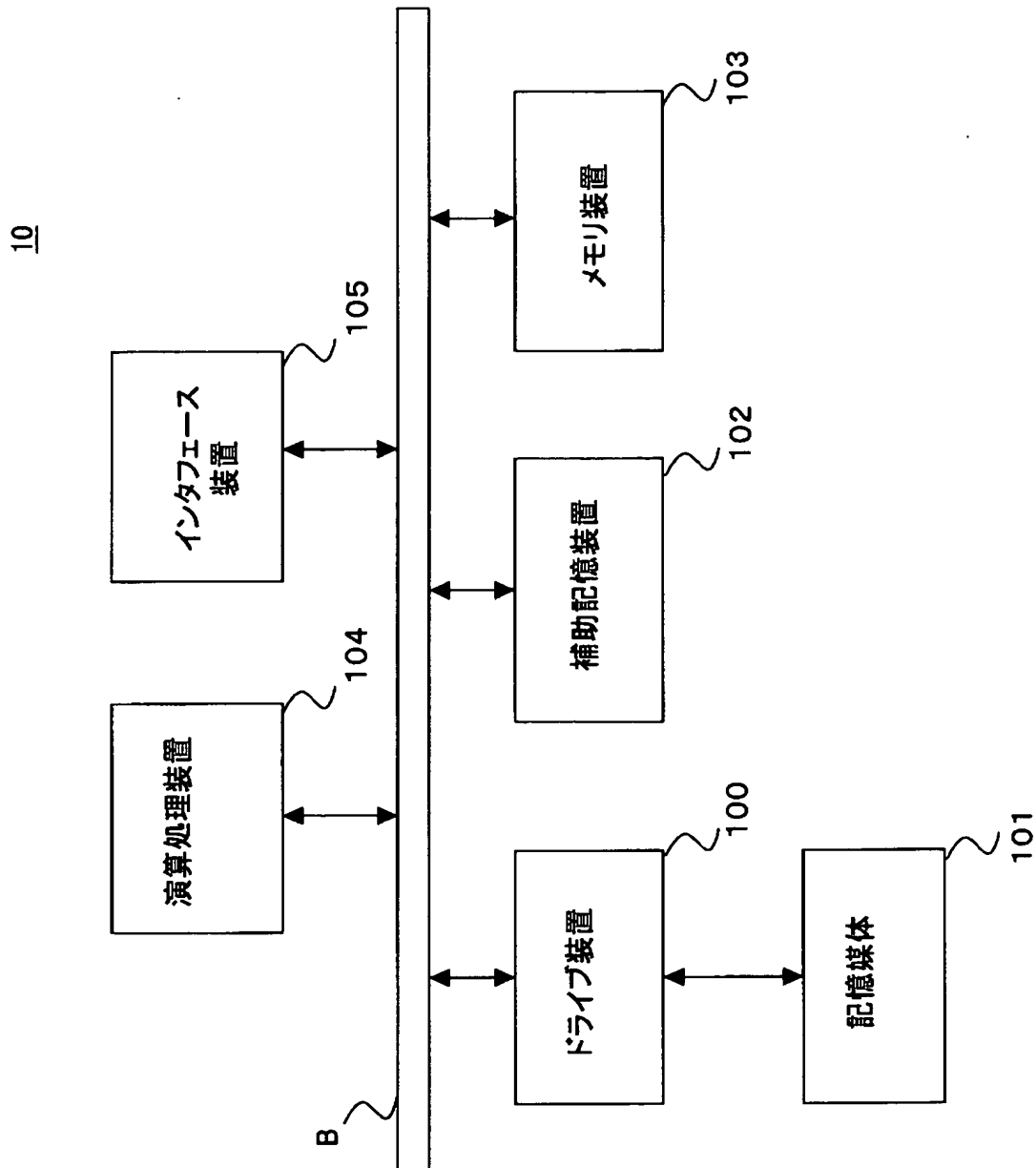
指紋DBを構成する指紋特徴データ管理テーブルの構成例を示す図

1821

ユーザID	指紋特徴データ
5551	<指紋特徴データ1>
5552	<指紋特徴データ2>
5553	<指紋特徴データ3>
:	:

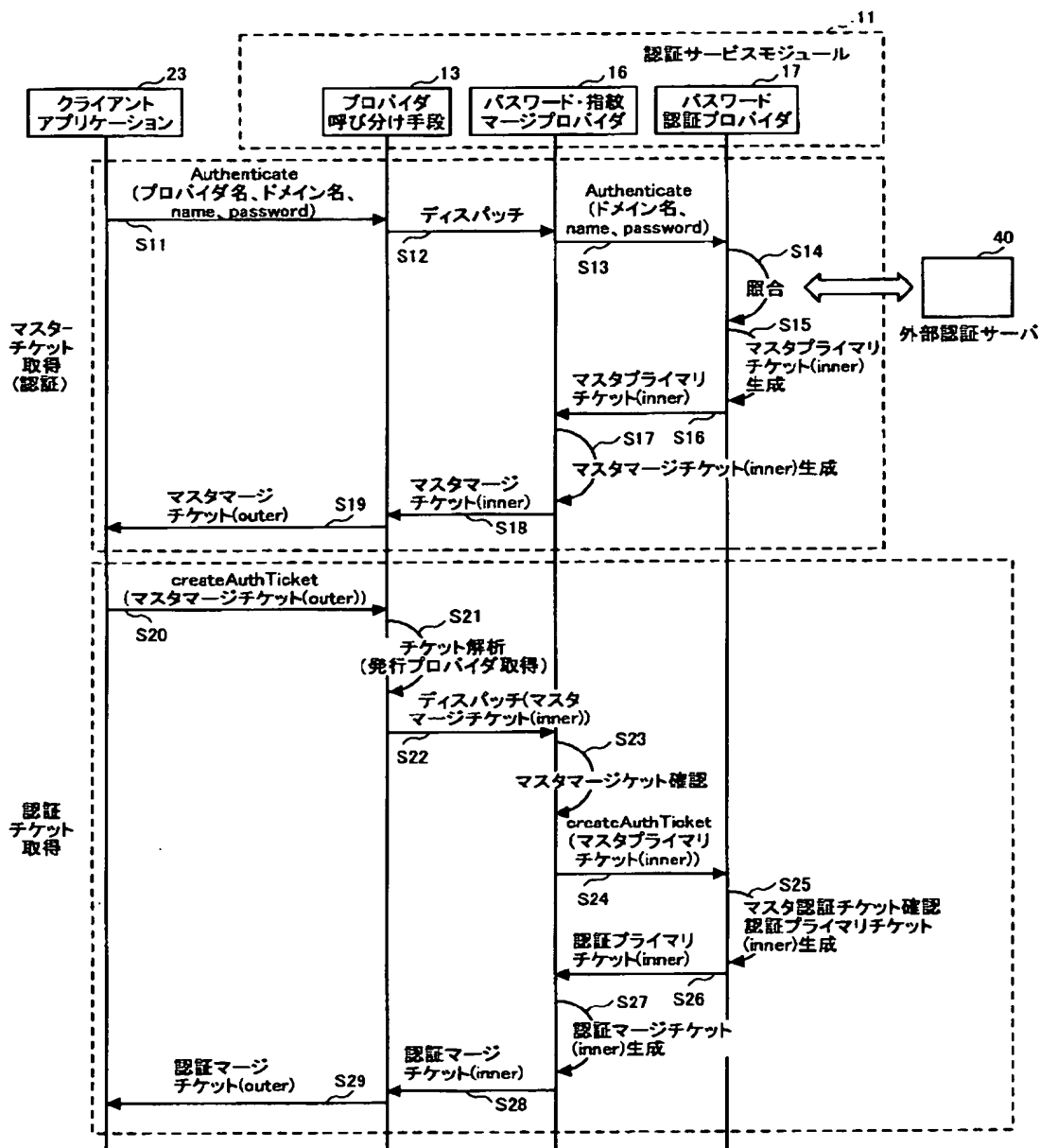
【図 8】

本発明の実施の形態における
認証サーバのハードウェア構成例を示す図



【図 9】

プライマリ認証の際の認証サーバの処理を
説明するためのシーケンス図



【図 1 0】

通常のチケットのデータ構造の例を示す図

501

チケットID
有効範囲
認証プロバイダ名
有効期限
認証ドメイン名
認証ユーザID
主なユーザ属性のリスト
MIC

【図 11】

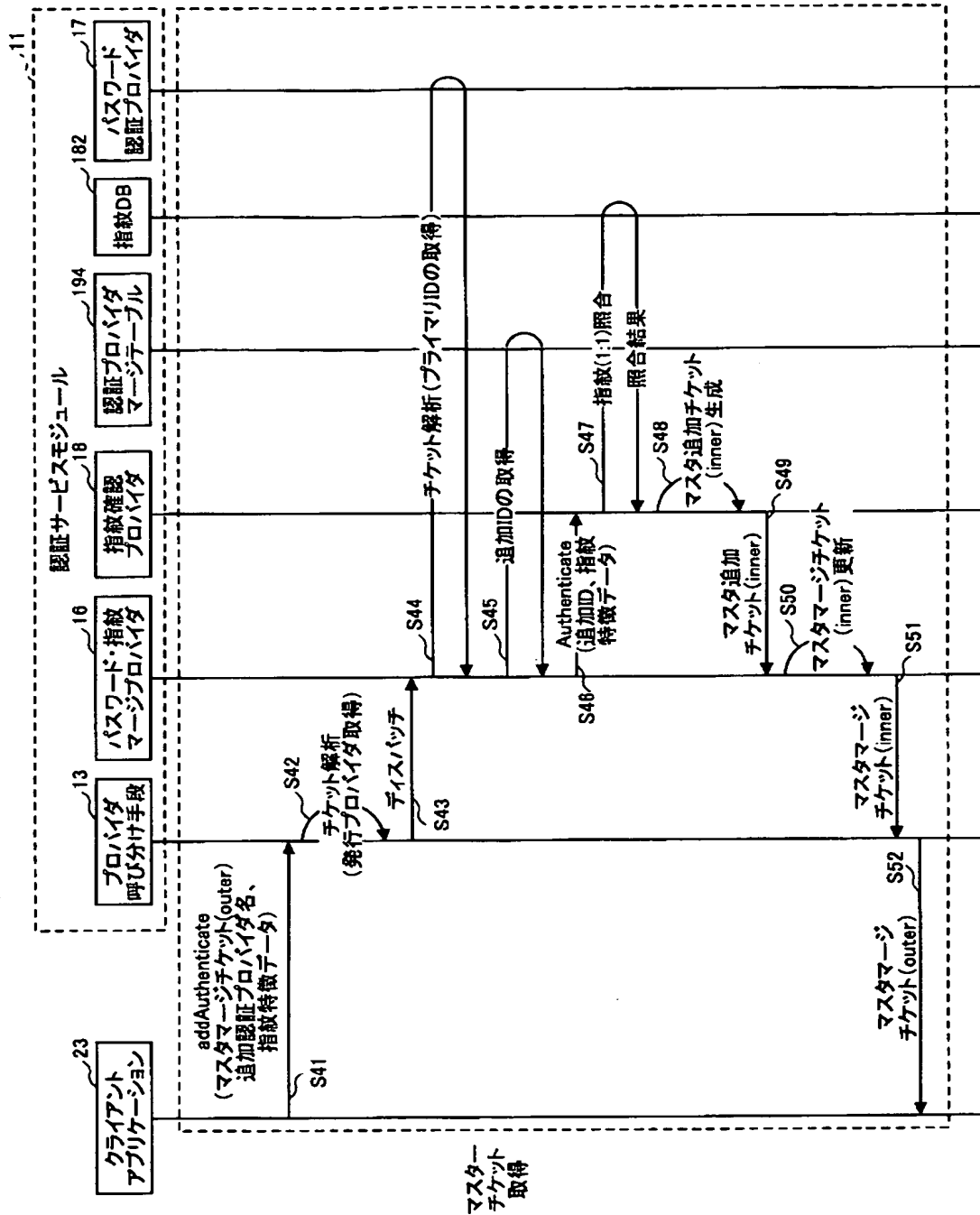
マージチケットのデータ構造の例を示す図

502

チケットID
チケット種別
認証プロバイダ名
有効期限
プライマリ認証プロバイダ名
プライマリチケット
追加チケットのリスト
MIC

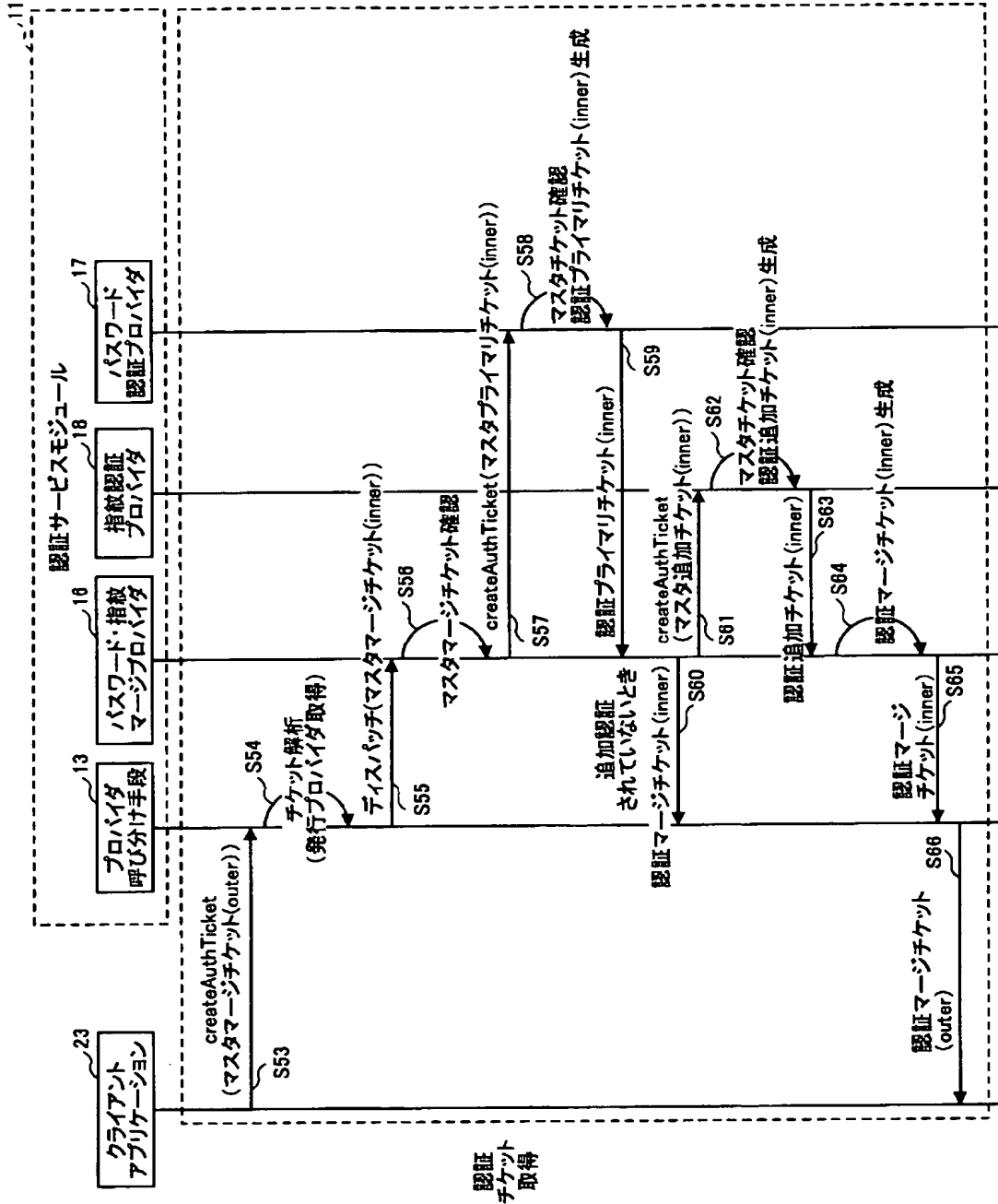
【図 12】

追加認証の際の認証サーバの処理を説明するためのシーケンス図



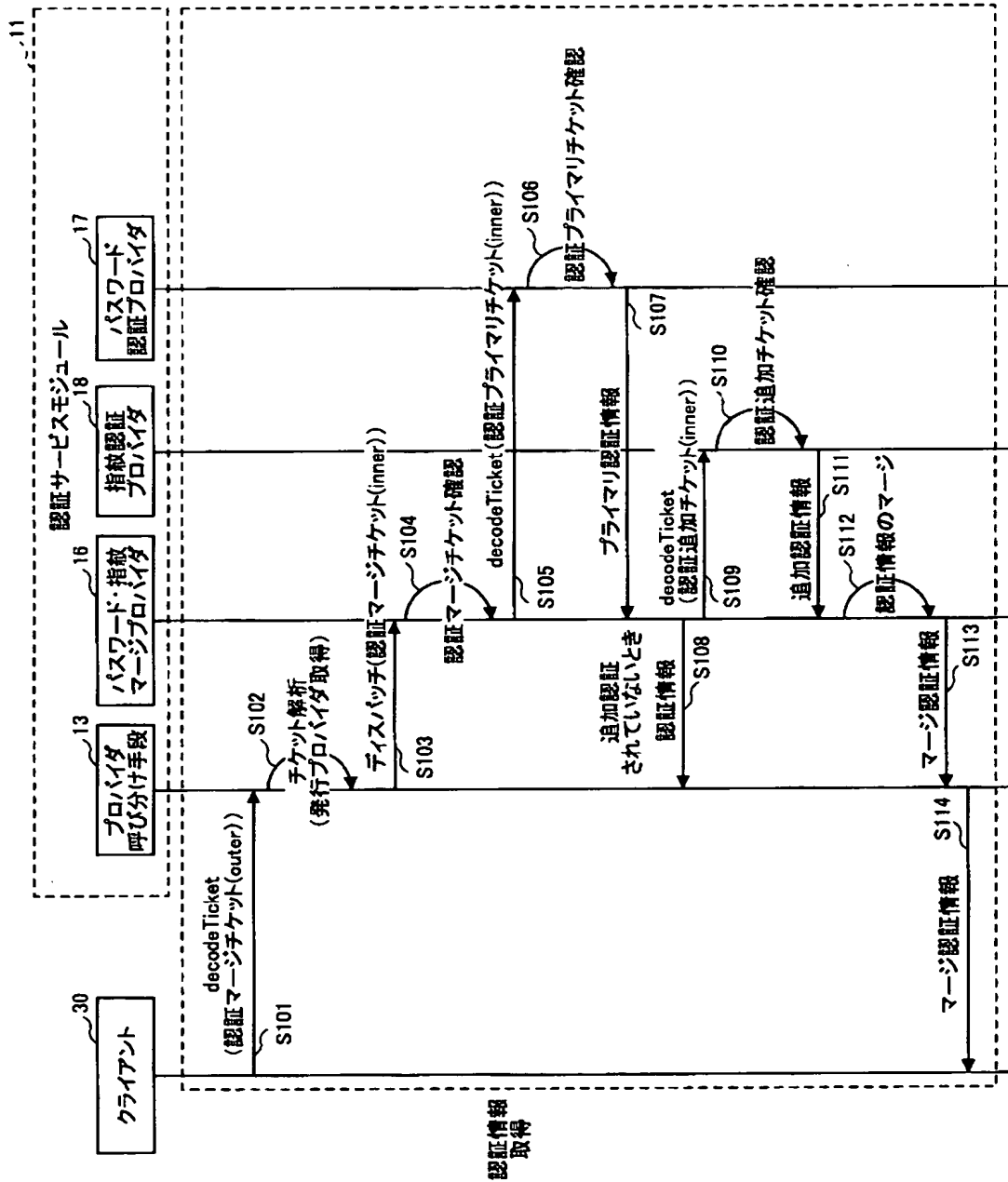
【図 13】

追加認証の際の認証サーバの処理を説明するためのシーケンス図



【図14】

チケットの第一の利用方法を説明するためのシーケンス図



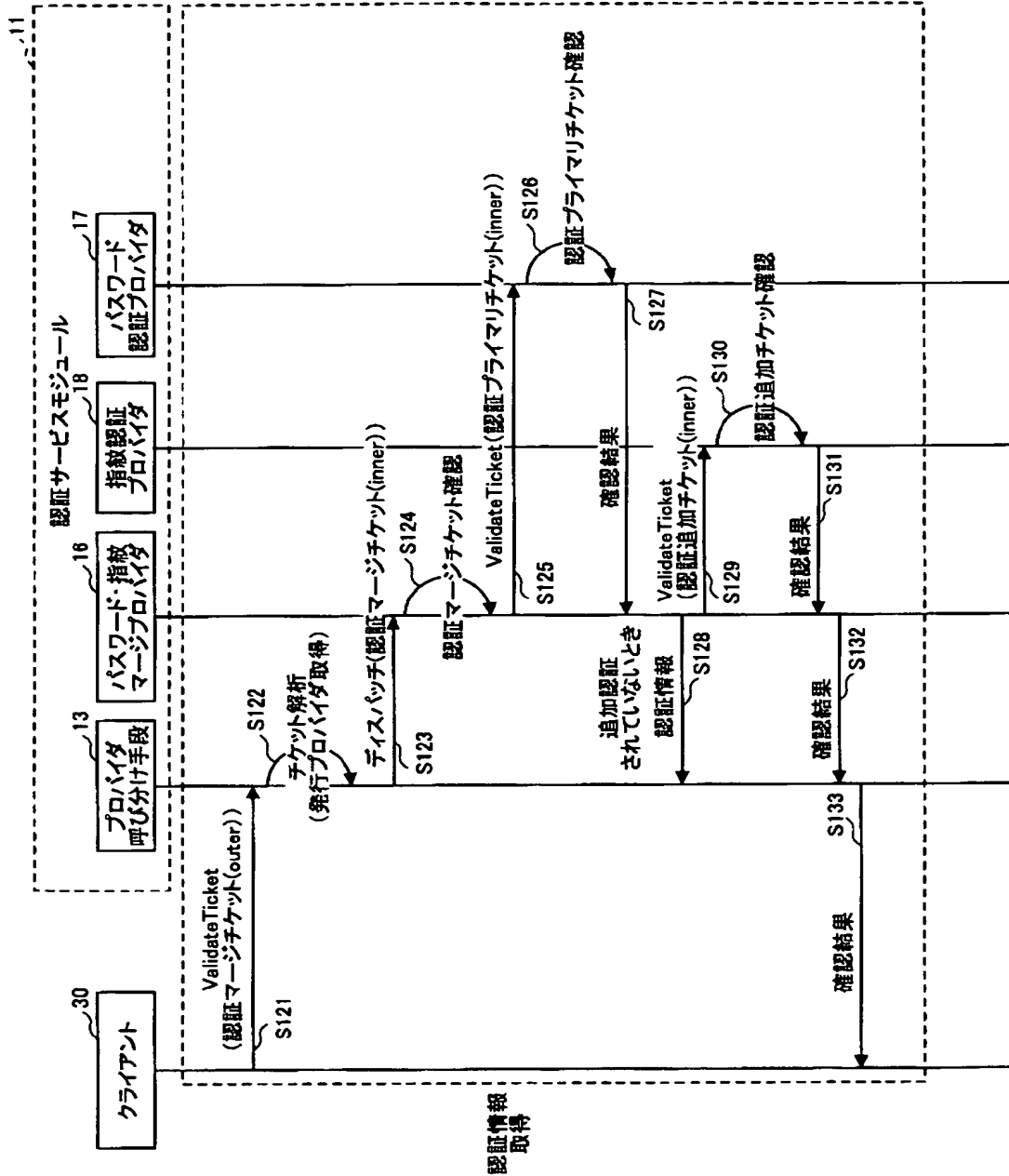
【図 15】

マージ認証情報データの構成例を示す図

認証サービス名	"UauthService01.RRR"
有効期限	2003/02/07:18:31:12
有効範囲	"サーバA"、"サーバB"
認証プロバイダ	"パスワード認証プロバイダ"、 "指紋認証プロバイダ"
ユーザ識別子	S-001-719964-772588612
所属グループ	Users, SscMembers, sgAdmin, fp_exclusive
主要属性	post=manager, class=AC, mail=xxx.rrr.co.jp

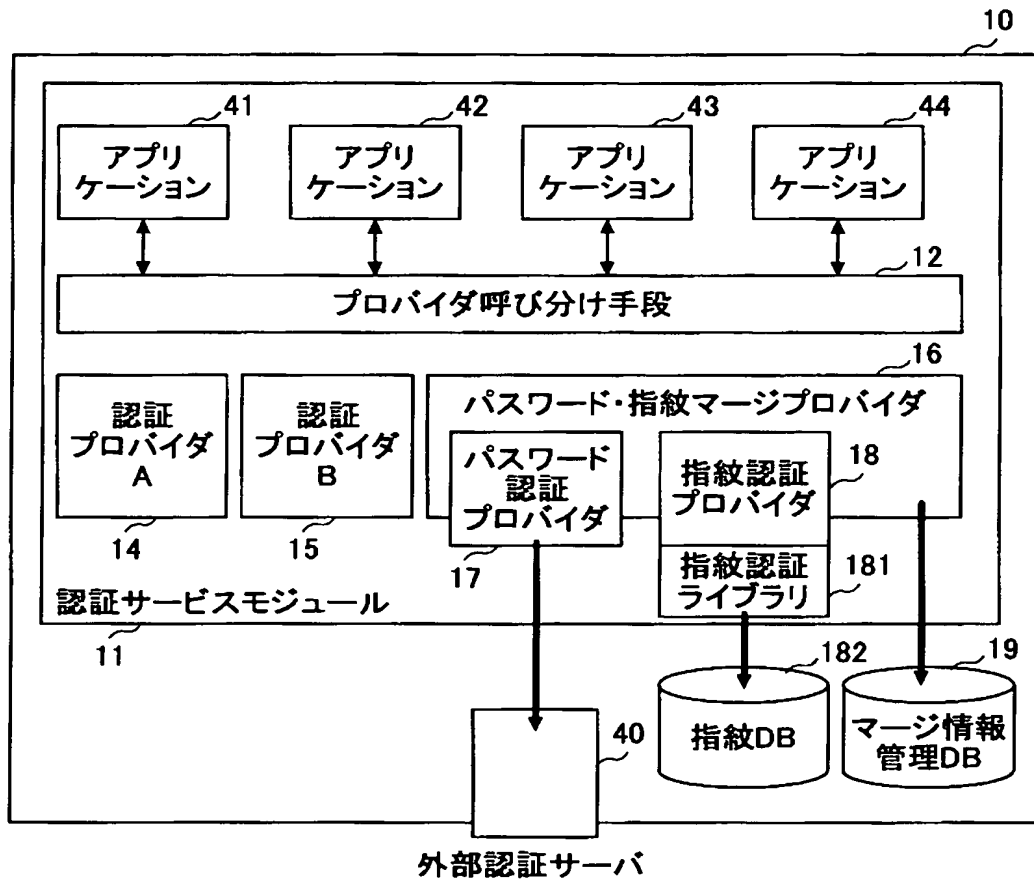
【図 16】

チケットの第二の利用方法を説明するためのシーケンス図



【図 17】

内部アプリケーションに認証機能を提供する場合の
認証サーバの機能構成例を示す図



【書類名】 要約書

【要約】

【課題】 ユーザの同一性を保証しつつ複数の認証機能によってユーザを認証することができるユーザ認証装置、ユーザ認証方法、ユーザ認証プログラム及び記録媒体の提供を目的とする。

【解決手段】 ユーザの認証を行う複数の認証手段を連携させる連携手段を有するユーザ認証装置であって、前記連携手段は、クライアントからのユーザの第一の認証要求に応じて、第一の認証手段に認証要求において指定された第一のユーザ識別情報に基づいてユーザを認証させる第一の呼び出し手段と、クライアントからの、第一の認証手段に認証されているユーザの第二の認証要求に応じて、第一のユーザ識別情報に予め対応づけられた、第二の認証手段におけるユーザの第二のユーザ識別情報を検索するユーザ識別情報検索手段と、第二の認証手段にユーザ識別情報検索手段が検索した第二のユーザ識別情報に基づいてユーザを認証させる第二の呼び出し手段とを有することにより上記課題を解決する。

【選択図】 図 1

特願 2003-078993

出願人履歴情報

識別番号

[000006747]

1. 変更年月日

2002年 5月17日

[変更理由]

住所変更

住 所

東京都大田区中馬込1丁目3番6号

氏 名

株式会社リコー